MISSISSIPPI LAW JOURNAL

SYMPOSIUM

THE FOURTH AMENDMENT: VIEWS OF THE FUTURE

SPONSORED BY THE

National Center for Justice and the Rule of Law

FOREWORD	*Thomas K. Cla*
BIG BROTHER OR LITTLE BROTHER? SURRENDERING SEIZURE PRIVACY FOR THE BENEFITS OF COMMUNICATION TECHNOLOGY	*José Felipé Anders*
A UNIFIED THEORY FOR SEIZURES OF THE PERSON	*Ronald Baci*
CHALLENGES TO *TERRY* FOR THE TWENTY-FIRST CENTURY	*Richard E. Myer*
WESTERN UNION, THE AMERICAN FEDERATION OF LABOR, GOOGLE, AND THE CHANGING FACE OF PRIVACY ADVOCATES	*Wesley MacNeil Oli*
THE NEW REALITY OF SEARCH ANALYSIS: FOUR TRENDS CREATED BY NEW SURVEILLANCE TECHNOLOGIES	*Ric Simmo*
THE WARREN COURT'S HOUSE BUILT ON SAND: FROM SECURITY IN PERSONS, HOUSES, PAPERS, AND EFFECTS TO MERE REASONABLENESS IN FOURTH AMENDMENT DOCTRINE	*Jack Wade Now*
RESPONDING TO THE CHALLENGES OF CONTEXTUAL CHANGE AND LEGAL DYNAMISM IN INTERPRETING THE FOURTH AMENDMENT	*Donald A. Dri*
REASONABLENESS WITH TEETH: THE FUTURE OF FOURTH AMENDMENT REASONABLENESS ANALYSIS	*Cynthia*
NO MORE CHIPPING AWAY: THE ROBERTS COURT USES AN AXE TO TAKE OUT THE FOURTH AMENDMENT EXCLUSIONARY RULE	*Tracey Macli* *Jennifer Ra*
FOURTH AMENDMENT FUTURE: REMOTE COMPUTER SEARCHES AND THE USE OF VIRTUAL FORCE	*Susan W. Bren*
THE FUTURE OF THE FOURTH AMENDMENT IN A DIGITAL EVIDENCE CONTEXT: WHERE WOULD THE SUPREME COURT DRAW THE ELECTRONIC LINE AT THE INTERNATIONAL BORDER?	*Patrick E. Corb*
THE FOURTH AMENDMENT IN A WORLD WITHOUT PRIVACY	*Paul O*
ELECTRONIC PRIVACY IN THE GOVERNMENT WORKPLACE AND *CITY OF ONTARIO, CALIFORNIA V. QUON*: THE SUPREME COURT BROUGHT FORTH A MOUSE	*Clifford S. Fishm*

Published by Students at the
University of Mississippi School of Law

Volume 81 **2012** **Number 5**

Digitized by the Internet Archive
in 2012 with funding from
LYRASIS Members and Sloan Foundation

http://archive.org/details/mississippilawjo81thom

Become a Friend of the *Mississippi Law Journal*

Today the *Mississippi Law Journal* is funded and operated almost exclusively through student efforts. Increasingly, however, the *Journal* depends on the support of its alumni and friends. You can become a Friend of the *Mississippi Law Journal* by making a tax-deductible contribution to one of the funds listed below. Checks should be made payable to the University of Mississippi Foundation and mailed to Post Office Box 8288, University, Mississippi 38677. *Please indicate on your check to which fund you intend to contribute.*

Robert C. Khayat Scholarship Endowment

The Robert C. Khayat Scholarship Endowment was established in 1995 to honor the dedicated service of Robert C. Khayat, a *Journal* alumnus, professor of law, and chancellor emeritus of the university. Each year the *Journal* awards the Robert C. Khayat scholarship to a deserving member.

Mississippi Law Journal Endowment

The *Mississippi Law Journal* Endowment exists to ensure the *Journal*'s future financial stability. As an entity financially independent of the school of law, the *Journal* depends partially on this endowment to fund its operations.

Mississippi Law Journal Operating Fund

All contributions to the *Mississippi Law Journal*'s operating fund help the *Journal* to meet its most immediate needs, including the cost of publication.

FRIENDS OF THE *MISSISSIPPI LAW JOURNAL**

DR. GUTHRIE T. ABBOTT
MRS. PAULA GRAVES ARDELEAN
THE HONORABLE RHESA H. BARKSDALE
MR. ROSS F. BASS JR.
MR. WILLIAM H. BECK JR.
BENNETT LOTTERHOS SULSER AND WILSON
THE HONORABLE WILLIAM H. BIZZELL
THE HONORABLE EUGENE M. BOGEN
MRS. TERI M. BOWIE
MRS. LORRAINE WALTERS BOYKIN
MR. JOHN R. BRALEY IV
MR. CHARLES L. BROCATO
MR. JASON W. BURCH
MR. JAMES T. CALDWELL
THE HONORABLE THAD COCHRAN
MR. RICHARD G. COWART
MR. T. DAVID COWART
MR. FRANK CROSTHWAIT JR.
MR. ARLEN B. COYLE
MR. WILLIAM M. DEAVOURS
MRS. MARLANE DOVE
MR. W. W. DRINKWATER JR.
DULIN & DULIN LTD.
LT. COMMANDER W.J. DUNAWAY
DR. WYLENE W. DUNBAR
MR. RICHARD M. EDMONSON SR.
MR. HERBERT C. EHRHARDT
DR. MARTHA JANE ELLIS
MR. ROGER M. FLYNT JR.
MR. WILLIAM M. GAGE
MR. ROBERT C. GALLOWAY
MRS. GRETCHEN L. GENTRY
MR. EUGENE B. GIFFORD JR.
MR. HAMPTON GLOVER JR.
MR. WILLIAM N. GRAHAM
MRS. LILLOWS ANN S. GRAYSON
MR. NEWT P. HARRISON
MR. ROBERT H. HODGES
MR. JAMIE G. HOUSTON III
MR. GARY K. JONES
MR. W.R. JONES JR.
MR. WILLIAM T. JONES
MRS. PATRICIA FLEMING KENNEDY
MR. WILLIAM N. KRUCKS
THE HONORABLE TOM STEWART LEE
MRS. VIRGINIA C. LOCOCO
MR. ROLAND MARBLE SR.
MR. M.C. MAXWELL
MS. LYDIA H. MCINTOSH
MR. JASON N. MCNEEL
MR. JOSEPH R. MEADOWS
MICHAEL T. & PAULINE S. LEWIS
MR. RUSSELL W. MILLS
MR. DAVID W. MOCKBEE
MR. H. DIXON MONTAGUE
MR. DALTON M. MOUNGER

Mrs. Trudy Lumpkin Muench
Mrs. Julie Sneed Muller
Mr. Christopher Tyson Nettles
Mr. James W. O'Mara
The Honorable J. D. Orlansky
Mr. Tom Ostenson
Mr. James A. Peden Jr.
Mr. Leroy D. Percy
Mr. Richard T. Phillips
Mr. Rubel L. Phillips
Mr. Benjamin J. Piazza Jr.
Mr. George B. Pickett Jr.
Mr. C. Michael Pumphrey
Mr. Clayton C. Purdom
Mr. Hollaman M. Raney
Mr. Eric Tyson Ray
Mr. Richard Roberts III
Mr. Lucius F. Sams Jr.
Ms. Lillous A. Shoemaker
Mr. George M. Simmerman Jr.
Mr. Jimmy Sledge Jr.
Mr. W. Marion Smith
Mr. Ronald T. Solberg
Mr. Darrell Solomon
Mr. Arthur D. Spratlin Jr.
Mrs. Patricia L. Stevens
Mr. Phineas Stevens
Mr. Samuel James Stigler
Mrs. Molly Fergusson Stuart
Mrs. Nancy H. Stumberg
Ms. Margaret J. Murphy Sweetland
Mr. Frank W. Trapp
Mr. Clint Douglas Vanderver
Mr. J. P. Varner
Mr. Lawrence D. Wade
Mrs. Michelle Clingan Waits
Mr. Tim Walsh
Mr. George D. Warner Jr.
Mr. Irwin G. Waterman
Mr. Louis H. Watson Jr.
Mr. Walker L. Watters
Dr. Robert A. Weems
Mr. Eddie C. Williams
Capt. Ronald J. Wojdyla

* *As of February 1, 2012*

The *Mississippi Law Journal* is published seven times during the academic year. The *Journal*'s editorial and business offices may be contacted via U.S. mail at: Post Office Box 849, University, Mississippi 38677.

Manuscripts: Manuscripts should be submitted electronically to **misslj@olemiss.edu**. Manuscripts should be in 12-point type and double-spaced, in Microsoft Word, WordPerfect, or PDF. Citations should conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (19th ed. 2010).

Subscriptions: $35.00 per year for domestic subscriptions; $40.00 per year for foreign subscriptions. Single issue: $15.00. Subscriptions are renewed automatically upon expiration unless the subscriber sends a notice of termination.

Change of address: Send address changes directly to the *Mississippi Law Journal*. Include name, new address (including zip code) and old address. Please notify the *Journal* forty-five days in advance to ensure prompt delivery.

Back Issues: Back issues of the *Mississippi Law Journal* may be ordered directly from William S. Hein & Co., Inc., 1285 Main Street, Buffalo, New York 14029-1987. Orders may also be placed by calling William S. Hein & Co., Inc., at (800) 828-7571, via fax at (716) 883-8100 or email to order@wshein.com. Back issues are available in PDF format through HeinOnline.

The *Mississippi Law Journal* is a member of the National Conference of Law Reviews. To offer its contributors complete freedom, the *Journal* assumes no responsibility for the views expressed herein.

Mississippi Law Journal

Published by Students at the
University of Mississippi School of Law

VOLUME 81 **2012** **NUMBER 5**

Copyright © 2012, Mississippi Law Journal, Inc.

Editor-in-Chief
BRENT COLE

Executive Editor
J. MORGAN STEPHENS

Executive Articles Editors
ALAN BAKER
MICHAEL BARBEE
LUKE CANTRELL
ADRIA HERTWIG
LOREN MCRAE

Notes & Comments Editors
ANDREW S. HARRIS
KATE VAN NAMEN

Business Manager
WILL CRAVEN

Executive Supra *Editor*
BRITTANY BARTLEY

Mississippi Cases Editor
PATRICK LOFTON

Associate Editors

Articles Editors
MICHAEL ATTAWAY
PARKER BERRY
ROBERT CAIN
ROBERT FORD
WES FRANCIS
CASSI FRANKS
KATHLEEN INGRAM
MARY JORDAN KIRKLAND
BRYAN SAWYERS
AUSTIN STOKES

Supra *Editors*
ELLIOTT FLAGGS
MATT SITTON

Mississippi Cases Editors
CHRISTINE BOCEK
JOHN CARRINGTON
JOSH DANIEL
ANDREW TOMINELLO

Technical Editor
APRIL H. KILLCREAS

Symposium Editor
JEFFREY BROWN

Notes & Comments Editor
ELIZABETH HYDE

Faculty Advisors
DEBORAH H. BELL
JOHN CZARNETZKY
ROBERT A. WEEMS

Staff Editors

Stephanie Jordan Bennett
Steven Bentley
Alex Bondurant
Travis Brackin
David Bunt
Susan Ellen Burgin
Emily Carroll
Risher Caves
Tulio D. Chirinos
Laura Elizabeth Collins
Charles Cowan
Sarah Dickey
Erin Doctor
M. Davidson Forester III
Haley Fowler
John Hensley
Whitney Holliday
Holly Hosford
Katherine Kimmel
Mary Kristen Kyle
Meagan Linton
R. Benjamin McMurtray
Grant Mullins
Evan Parrott
Erica Peden
Cody Roebuck
Warren A. Stafford
Emily Logan Stedman
Anna Sweat
Kimberly Thompson
Jack West
Brian Whitman
Michael Williams
Suneisha Williams

Administrative Officers of the University of Mississippi

Daniel W. Jones	*Chancellor*
Morris H. Stocks	*Provost and Vice Chancellor for Academic Affairs*
Alice M. Clark	*Vice Chancellor for Research and Sponsored Programs*
Larry D. Sparks	*Vice Chancellor for Administration and Finance*
Wendell Weakley	*President and CEO, The University of Mississippi Foundation*
Andrew P. Mullins Jr.	*Chief of Staff to the Chancellor*
Timothy L. Walsh	*Executive Director of Alumni Affairs*
I. Richard Gershon	*Dean of the School of Law and Professor of Law*

The Law School Faculty

Guthrie T. Abbott, *Professor Emeritus of Law and Butler, Snow, O'Mara, Stevens and Cannada Lecturer in Law Emeritus*

Michele Alexandre, *Assistant Professor of Law*

Richard L. Barnes, *Professor of Law and Leonard B. Melvin, Jr. Distinguished Lecturer in Law*

Deborah H. Bell, *Professor of Law and Mississippi Defense Lawyers Association Distinguished Lecturer in Law*

William W. Berry III, *Assistant Professor of Law*

Percy J. Blount, *Research Counsel and Instructor, National Center for Remote Sensing, Air and Space Law*

John R. Bradley Jr., *Professor of Law*

Phillip W. Broadhead, *Director, Clinical Appeals Program and Clinical Professor of Law*

Charles Brower II, *Croft Professor of International Law and Jessie D. Puckett, Jr. Lecturer in Law*

Mercer E. Bullard, *Associate Professor of Law*

Larry Bush, *Professor Emeritus of Law*

W. Tucker Carrington, *Director, Mississippi Innocence Project*

David W. Case, *Associate Professor of Law*

Thomas K. Clancy, *Director of the National Center for Justice and the Rule of Law and Research Professor of Law*

George C. Cochran, *Professor of Law*

Aaron S. Condon, *Professor Emeritus of Law*

Benjamin P. Cooper, *Assistant Professor of Law*

John M. Czarnetzky, *Professor of Law and Mitchell, McNutt, and Sams Lecturer*

Donna Davis, *Associate Professor of Law*

Samuel M. Davis, *Jamie L. Witten Chair of Law and Government and Professor of Law*

Jason Derrick, *Acting Assistant Professor of Legal Writing*

D. Michael Featherstone, *Professor Emeritus of Law*

Molly Fergusson, *Acting Assistant Professor of Legal Writing*

Don L. Fruge, *Professor Emeritus and President and CEO Emeritus of the University of Mississippi Foundation*

Joanne I. Gabrynowicz, *Director of the National Remote Sensing, Air and Space Law Center and Research Professor of Law*

Kris L. Gilliland, *Director of Law Library and Associate Professor of Law*

Christopher R. Green, *Assistant Professor of Law*

Karen O. Green, *Professor of Law and Mississippi Defense Lawyers Association Distinguished Lecturer in Law*

Matthew R. Hall, *Associate Dean for Academic Affairs, Associate Professor of Law and Jessie D. Puckett, Jr., Lecturer*

Desiree Hensley, *Assistant Professor of Law and Director of Civil Legal Clinic*

Michael H. Hoffheimer, *Professor of Law and Mississippi Defense Lawyers Association Distinguished Lecturer in Law*

Robert C. Khayat, *Chancellor Emeritus and Professor Emeritus of Law*

Patricia Krueger, *Acting Assistant Professor of Legal Writing and Director of Academic Excellence Program*

Don Mason, *Associate Director of the National Center for Justice and the Rule of Law and Lecturer*

Gary Myers, *Professor of Law and Associate Dean for Research*

Jack W. Nowlin, *Associate Professor of Law and Jessie D. Puckett, Jr., Lecturer*

Niki Pace, *Research Counsel, Mississippi-Alabama Sea Grant*

E. Farish Percy, *Associate Professor of Law and Jessie D. Puckett, Jr., Lecturer*

Larry J. Pittman, *Professor of Law and Jessie D. Puckett, Jr., Lecturer*

Lisa S. Roy, *Associate Professor of Law and Jessie D. Puckett, Jr., Lecturer*

Ronald J. Rychlak, *Professor of Law and Mississippi Defense Lawyers Association Lecturer in Law*

Jacqueline Serrao, *Associate Director and Instructor, National Remote Sensing, Air and Space Law Center*

Stephanie Showalter-Otts, *Director of the National Sea Grant Law Center and Adjunct Professor of Law*

Hans P. Sinha, *Director of Prosecutorial Externship Program and Clinical Professor of Law*

Carolyn Ellis Staton, *Provost Emeritus and Professor Emeritus of Law*

Robert A. Weems, *Professor of Law and Butler, Snow, O'Mara, Stevens and Cannada Lecturer in Law*

Will Wilkins, *Director of the Mississippi Law Research Institute*

C. Jackson Williams, *Director of Legal Writing Program and Acting Assistant Professor of Legal Writing*

Parham H. Williams Jr., *Dean Emeritus and Professor Emeritus of Law*

MISSISSIPPI LAW JOURNAL
Published by Students at
The University of Mississippi School of Law

VOLUME 81 2012 NUMBER 5

TABLE OF CONTENTS

ARTICLES

FOREWORD

.... *Thomas K. Clancy* i

The Future of Seizure Analysis

BIG BROTHER OR LITTLE BROTHER? SURRENDERING SEIZURE PRIVACY FOR THE BENEFITS OF COMMUNICATION TECHNOLOGY

.... *José Felipé Anderson* 895

A UNIFIED THEORY FOR SEIZURES OF THE PERSON

.... *Ronald Bacigal* 915

CHALLENGES TO *TERRY* FOR THE TWENTY-FIRST CENTURY

.... *Richard E. Myers II* 937

The Future of Search Analysis

WESTERN UNION, THE AMERICAN FEDERATION OF LABOR, GOOGLE, AND THE CHANGING FACE OF PRIVACY ADVOCATES

.... *Wesley MacNeil Oliver* 971

THE NEW REALITY OF SEARCH ANALYSIS: FOUR TRENDS CREATED BY NEW SURVEILLANCE TECHNOLOGIES

.... *Ric Simmons* 991

What the Amendment Protects: "Security" in the Twenty-First Century

THE WARREN COURT'S HOUSE BUILT ON SAND: FROM SECURITY IN PERSONS, HOUSES, PAPERS, AND EFFECTS TO MERE REASONABLENESS IN FOURTH AMENDMENT DOCTRINE

.... *Jack Wade Nowlin* 1017

The Future of "Reasonableness" Analysis: When is a Search or Seizure Justified?

RESPONDING TO THE CHALLENGES OF CONTEXTUAL CHANGE AND LEGAL DYNAMISM IN INTERPRETING THE FOURTH AMENDMENT

.... *Donald A. Dripps* 1085

REASONABLENESS WITH TEETH: THE FUTURE OF FOURTH AMENDMENT REASONABLENESS ANALYSIS

....*Cynthia Lee* 1133

The Exclusionary Rule

NO MORE CHIPPING AWAY: THE ROBERTS COURT USES AN AXE TO TAKE OUT THE FOURTH AMENDMENT EXCLUSIONARY RULE

....*Tracey Maclin & Jennifer Rader* 1183

The Future of Digital Evidence Searches and Seizures

FOURTH AMENDMENT FUTURE: REMOTE COMPUTER SEARCHES AND THE USE OF VIRTUAL FORCE

.... *Susan W. Brenner* 1229

THE FUTURE OF THE FOURTH AMENDMENT IN A DIGITAL EVIDENCE CONTEXT: WHERE WOULD THE SUPREME COURT DRAW THE ELECTRONIC LINE AT THE INTERNATIONAL BORDER?

....*Patrick E. Corbett* 1263

THE FOURTH AMENDMENT IN A WORLD WITHOUT PRIVACY

....*Paul Ohm* 1309

THE JAMES OTIS LECTURE

INTRODUCTION TO THE JAMES OTIS LECTURE

.... *Thomas K. Clancy* 1357

ELECTRONIC PRIVACY IN THE GOVERNMENT WORKPLACE AND *CITY OF ONTARIO, CALIFORNIA V. QUON*: THE SUPREME COURT BROUGHT FORTH A MOUSE

.... *Clifford S. Fishman* 1359

FOREWORD

THE FOURTH AMENDMENT: VIEWS OF THE FUTURE

Celebrating 10 Years of Symposia

2011 FOURTH AMENDMENT SYMPOSIUM

*Thomas K. Clancy**

The National Center for Justice and the Rule of Law,[1] which is a program of the University of Mississippi School of Law, focuses on issues relating to the criminal justice system, with its purpose to promote the two concepts comprising the title of the Center. In furtherance of its mission, the Center has established the *Fourth Amendment Initiative*. The purpose of the Center's initiative is to promote awareness of Fourth Amendment principles through conferences, publications, and training of professionals in the criminal justice system. The Center takes no point of view as to the direction that Fourth Amendment analysis should take but seeks to facilitate awareness of the issues and encourage discussion of search and seizure principles.

---

* Director, National Center for Justice and the Rule of Law, and Research Professor, University of Mississippi School of Law.

[1] The National Center for Justice and the Rule of Law is supported by a grant from the Bureau of Justice Assistance, Office of Justice Programs, of the U.S. Department of Justice. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in the articles stemming from this symposium are those of the author and do not represent the official position of the United States Department of Justice. For more information about the Center, please visit www.ncjrl.org.

A central pillar of the Fourth Amendment Initiative is its annual symposium on important search and seizure topics. 2011 was our 10th year of hosting symposia and the Center took that occasion to ask Fourth Amendment scholars to look to the future and offer perspectives on how search and seizure principles will or should develop. The symposium is roughly divided into six topics. Four of the topics mimic essential terms of the Fourth Amendment: "seizures"; "searches"; the right to be "secure"; and the concept of "unreasonable." Professor Tracey Maclin then follows with an article that adds perspective on the exclusionary rule. The final group of topics examines what is rapidly becoming the most common form of a search or seizure–obtaining digital evidence from the ubiquitous devices that characterize modern life.

The authors in this volume of the *Mississippi Law Journal* offer an extensive treatment of the future. The symposium was the second day of an appellate judge conference on selected Fourth Amendment topics. In the audience were approximately forty-five appellate judges from across the country, as well as academics, members of the law school community, and others. It was webcast and the recorded presentations may be viewed at www.NCJRL.org. I thank the authors for contributing to the symposium and to furthering our knowledge of Fourth Amendment jurisprudence.

BIG BROTHER OR LITTLE BROTHER? SURRENDERING SEIZURE PRIVACY FOR THE BENEFITS OF COMMUNICATION TECHNOLOGY

*José Felipé Anderson**

INTRODUCTION 896
I. THE *KRAMER* DECISION 901
II. WHY IS THE *KRAMER* DECISION IMPORTANT FOR THE FUTURE? 907
CONCLUSION 912

> They that can give up essential liberty to obtain a little temporary safety deserve neither safety nor liberty.[1]
>
> Benjamin Franklin

> O cruel, needless misunderstanding! . . . But it was all right, everything was all right, the struggle was finished. He had won the victory over himself. He loved Big Brother.[2]
>
> George Orwell

---

* Professor of Law and Founding Director Stephen L. Snyder Center for Litigation Skills (2000-2008) University of Baltimore School of Law. Adjunct Professor of Legal Studies and Business Ethics, The Wharton School, University of Pennsylvania. Research funding for this work was underwritten by the National Center for Justice and the Rule of Law at the University of Mississippi School of Law, which is supported by a grant from the Bureau of Justice Assistance, Office of Justice Programs at the U.S. Department of Justice. The author acknowledges Professor Thomas K. Clancy, Director of the National Center for Justice and the Rule of Law, the faculty, panel participants, appellate judges and students of the University of Mississippi School of Law who attended a lecture and discussion of an earlier draft of this paper, and for the many helpful suggestions that resulted.

[1] Benjamin Franklin, *Reply of the Pennsylvania Assembly to the Governor (Nov. 1755)*, *in* POWER QUOTES 106 (Daniel B. Baker ed., 1992).

[2] GEORGE ORWELL, 1984 at 266 (Plume 1983) (1949).

INTRODUCTION

Over two centuries have passed since Benjamin Franklin quipped that we should defend privacy over security if people wanted either privacy or security.[3] Although his axiom did not become a rule of law in its original form, its principles found voice in the Fourth[4] and Fifth[5] Amendments of the Constitution's Bill of Rights.[6] To a lesser extent, provisions against the quartering of troops in private homes found in the Third Amendment[7] also support the idea that what a government can require you to do, or who you must have behind the doors of your home, is an area of grave importance for privacy purposes.[8] By our behavior as a nation, have we indicated a rejection of the liberty Franklin was writing about in our modern times? In no area has the rapid rise of technology affected our lives more than in the area of communication through computers and other devices, like so-called "smart telephones."[9]

---

[3] Franklin, *supra* note 1.

[4] The Fourth Amendment of the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV. One Fourth Amendment historian has explained that the:

> Amendment provides that if there is to be a search and seizure, it must be a reasonable one. The only absolute standard that is set is as to the essentials of a warrant when such is necessary, as it is in most cases. The purpose of the latter part of the Amendment of course is to safeguard against the general warrant and it does this in two ways: first, by prescribing the requirement of probable cause, necessarily peculiar to each case; and second, by making requisite the description of the particular place to be searched, the persons to be apprehended, and the objects to be seized. These requirements limit the scope of each warrant; they take the decision as to what may and what may not be done out of the hands of the officer who is to execute the warrant, and place it with the more trustworthy and sober judgment of a judicial officer. It is for the latter to pass upon the merits of the allegations and, on the basis of evidence having behind it the responsibility of an oath, to decide whether there is reasonable justification for this exceptional proceeding in invasion of the individual's privacy, and thus to determine what particular actions are justified on the basis of this showing. There is no temptation for the ministerial officer to exceed the authority which the magistrate decides to give him, for he not only thereby subjects himself to civil and criminal liability but gains no advantage over the accused and merely wastes his effort.

NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 120 (1937) (footnote omitted).

[5] U.S. CONST. amend. V.

[6] One Supreme Court Justice has said:

> [T]he concepts of privacy which the Founders enshrined in the Fourth Amendment vanish completely when we slavishly allow an all-powerful government, proclaiming law and order, efficiency, and other benign purposes, to penetrate all the walls and doors which men need to shield them from the pressures of a turbulent life around them and give them health and strength to carry on.

United States v. White, 401 U.S. 745, 756 (1971) (Douglas, J., dissenting).

[7] "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law." U.S. CONST. amend. III.

[8] In *Camara v. Municipal Court*, 387 U.S. 523, 529 (1967), the Supreme Court said:

> The right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance. When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or government enforcement agent.

Id. (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)) (internal quotation marks omitted). The Fourth Amendment reflects critical values. "Indeed, these rights are so strong that the Constitution prohibits the most minimal transgressions against them. . . . Personal security, liberty, and private property are not discrete interests; they unite to define significant attributes of individual freedom in the democracy." Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 576 (1996).

[9] So-called smart phone technology has made it possible to perform many communications functions in a small device when such tools were unimaginable only a few years ago. The Supreme Court has already demonstrated a willingness to allow technology, such as tracking devices, to evade constitutional scrutiny. *See* United States v. Knotts, 460 U.S. 276, 285 (1983) (holding that placing a beeper type location device, without a warrant, in a barrel of contraband is not a search under the Fourth Amendment). It is unlikely that the Court desires to get involved in the day-to-day regulation of emerging technology. Most recently, the Supreme Court clarified its view on high technology searches in *United States v. Jones*, where it held that the government's use of a Global Positioning System on a private vehicle to monitor its movements constituted a search under the Fourth Amendment, therefore requiring a warrant to be obtained. *See* 132 S. Ct. 945 (2012). The *Jones* case seems curiously in conflict with the Court's prior holding in *Knotts*—invalidating the warrantless search—in that Justice Scalia's opinion pointed out that the "government physically occupied private property for the purpose of obtaining information." *Jones*, 132 S. Ct. 945, 949. Harkening back to the colonial days when horse and carriage was the primary mode of on-road transportation, the Justice reasoned that the intrusion in *Jones* was no different than "a constable's concealing himself in the target's coach in order to track its movements." *Jones*, 132 S. Ct. at 950 n.3. It remains to be seen

As long as people have been communicating, there has been a desire for others to be interested in hearing what they say.[10] Sometimes the speaker or writer desires an audience and the speaker's freedom to communicate desires protection.[11] At other times, people intend to keep their private words private while others desire to know their thoughts and intentions. This human desire, the "right to be let alone,"[12] has both practical and legal limitations. Obviously society has its own right to protect its members from violence and keep the peace by legislating and

---

whether this opinion signals any movement toward the Supreme Court extending greater privacy from technology-assisted searches. It only hinted in the opinion that it "may eventually have to grapple with these 'vexing problems' in some future cases . . . ." *Jones*, 132 S. Ct. at 954. Currently, such conflicting opinions on intrusion technology when the Supreme Court takes on such cases do not provide ample guidance as technology advances. In my view these occasional rulings on such searches will do little to provide more privacy.

[10] The most familiar area of electronic intrusion that courts have addressed is wiretapping. But such surveillance, that is, listening in secret, is an ancient practice. As one court recently explained:

> Eavesdropping is an ancient practice which at common law was condemned as a nuisance. At one time the eavesdropper listened by naked ear under the eaves of houses or their windows, or beyond their walls seeking out private discourse. The awkwardness and undignified manner of this method as well as its susceptibility to abuse was immediately recognized. Electricity, however, provided a better vehicle and with the advent of the telegraph surreptitious interception of messages began. As early as 1862[,] California found it necessary to prohibit the practice by statute. During the Civil War General J.E.B. Stuart is reputed to have had his own eavesdropper along with him in the field whose job it was to intercept military communications of the opposing forces. . . .
>
> The telephone brought on a new and more modern eavesdropper known as the 'wiretapper.' Interception was made by a connection with a telephone line.

Kopko v. Miller, 842 A.2d 1028, 1034 (Pa. Commw. Ct. 2004) (quoting Berger v. New York, 388 U.S. 41, 45-46 (1967)).

[11] "In time, given the global movement toward democracy, interactive voice, audio, video data exchange will occur world wide. In addition to fiber optics, dozens of other technological innovations will end our dependency on the electromagnetic spectrum." JONATHAN W. EMORD, FREEDOM, TECHNOLOGY AND THE FIRST AMENDMENT 308 (1991).

[12] The right to be let alone by government officials, unless there exists sufficient cause, is protected by the Fourth Amendment. This right is "perhaps the most personal of all legal principles. It is also one of the newest, since only the more sophisticated of societies have the interest and the ability to nurture that subtle and most personal possession of man, his dignity." MORRIS L. ERNST & ALAN U. SCHWARTZ, PRIVACY: THE RIGHT TO BE LET ALONE 1 (1962).

enforcing criminal law.[13] When technology comes into existence, law enforcement often uses it first to engage in the "competitive enterprise [to] ferret[] out crime."[14] Further, the technology itself may make it impossible to permit people who desire to keep information private from achieving that goal. Among the reasons that keeping matters private has become more difficult is that the law simply cannot keep up with the rapid rise in communications technology.[15]

The rise in technology is not a new issue;[16] what is new is our willingness to surrender control of how our personal information is stored and accessed in the face of our desire for the convenience that communications technology offers. It is that topic on which this Article focuses. This commentary is not intended to be an extensive review of any aspect of the debate over privacy and technology. Indeed, my purpose is to make thoughtful people ask questions about how comfortable they have become with the mass of easily accessible personal information stored by so many entities.

---

[13] *See Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. 78 (2000) (statement of Kevin V. DiGregory, Deputy Assoc. Att'y Gen. DOJ). "Carnivore is '[e]ssentially a personal computer stuffed with specialized software, [which] represents a new twist in the federal government's fight to sustain its snooping powers in the Internet age.' The *Wall Street Journal* also reported that Carnivore 'can scan millions of e-mails a second' . . . ." Trenton C. Haas, *Carnivore and the Fourth Amendment*, 34 CONN. L. REV. 261, 261 (2001) (alteration in original) (footnote omitted) (quoting Neil King, Jr. & Ted Bridis, *FBI's Wiretaps to Scan E-mail Spark Concern*, WALL ST. J., July 11, 2000, at A3).

[14] Johnson v. United States, 333 U.S. 10, 14 (1948).

[15] The ability of government to intrude electronically increases each day as technology advances. Without statutory controls, it is likely that fewer areas of our lives can be kept private. One insightful commentator has explained that:

> [E]lectronic surveillance is almost inherently indiscriminate. Interception of a telephone line provides to law enforcement all of the target's communications, whether they are relevant to the investigation or not, raising concerns about compliance with the particularity requirement in the Fourth Amendment and posing the risk of general searches. In addition, electronic surveillance involves an on-going intrusion in a protected sphere, unlike the traditional search warrant, which authorizes only one intrusion, not a series of searches or a continuous surveillance. Officers must execute a traditional search warrant with dispatch, not over a prolonged period of time. If they do not find what they were looking for in a home or office, they must leave promptly and obtain a separate order if they wish to return to search again. Electronic surveillance, in contrast, continues around-the-clock for days or months. Finally, the usefulness of electronic surveillance depends on lack of notice to the suspect.

James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 70 (1997) (footnotes omitted).

[16] Professor Arthur Miller, in a prophetic statement about a quarter of a century ago, framed the challenge of the courts' role in privacy protection and the challenges that courts and society would face as we anticipated the promise of the high technology age. He wrote:

These disputes about privacy, like all critical legal disputes unaddressed by the legislature, will find their way to the nation's courts. We can fully expect that the future will bring more disputes into the judicial system as more technology is created, impacting our private information and bringing new meaning to the often-used expression that "Big Brother is watching."[17] One such dispute recently made its way to court in a somewhat unusual way, emerging as a sentencing issue in a child sexual abuse case, rather than a motion to suppress evidence alleged to be illegally seized in a criminal prosecution.[18] In the case of

---

> The notion that the courts will recognize a general principle requiring data handlers to treat personal information as confidential or will declare that file keepers owe a fiduciary duty to file subjects seems to be wishful thinking. Nor is it realistic to think that a pledge of confidentiality can be secured on a contractual basis. In most situations involving data extraction, the individual is in no position to demand a promise to this effect. Of course, the courts may change their attitude when the potentialities of the computer become apparent. But to wait for the courts to create common-law obligations and impose them on information extractors, processors, transmitters, and users for the benefit of data subjects will require the patience of Job and may prove to be no more fruitful than agitating for the expansion of the common-law privacy action. Time is a luxury personal privacy cannot afford and the glacial movement of legal doctrine is inappropriate for the problem at hand.

ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 220 (1971).

[17] One insightful commentator has recognized that the "advent of widespread use of computer technology . . . has altered the way in which individuals view the world . . . . Today, lawyers and business professionals must be cognizant of communications law, criminal law, privacy law, and many other subjects that may not have been relevant to their situation only a decade ago." RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY: RIGHTS, LICENSES, LIABILITIES, III-1 (2d ed. 1992).

[18] The so-called exclusionary rule has had its critics. Almost two decades after the exclusionary rule had been adopted in *Mapp v. Ohio*, 367 U.S. 643 (1961), President Ronald Reagan established a commission which recommended it be abolished. In its report, the task force explained:

United States v. Kramer, a federal appellate court was asked to decide whether a telephone used in committing the crime at issue was a "computer."[19]

I. THE *KRAMER* DECISION

In what can be fairly described as an opinion that centered on only one definition that will no doubt affect many, a court was asked to categorize a cellular telephone as a computer, as described in certain federal criminal statutes.[20] The troubling facts involved Neil Kramer's conviction of a crime against a fifteen-year-old female from Missouri who inadvertently sent a text message to Kramer's phone, beginning a seven-month period of "text messaging and telephonic communication."[21] Kramer was made aware of the victim's age.[22] In November of 2008, Kramer met the victim at a Missouri convenience store after driving from his home in Louisiana.[23] "The pair drove to the Comfort Inn in Willow Springs, Missouri, where he plied the victim with illegal narcotics and then engaged in sexual intercourse with her."[24] The day after their first sexual encounter, the victim was transported to Kramer's trailer located in Violet, Louisiana. On Friday 14, 2008, the victim was able to text her mother, reporting her location from a Louisiana bar.[25] Members of the St. Bernard Parish Sherriff's Department responded to the bar.[26] Kramer was

---

> Legislation should be proposed and enacted to abolish the exclusionary rule as it is applies to Fourth Amendment issues. . . . Anyone evaluating the exclusionary rule must constantly keep this basic premise in mind. The framers of the Constitution did not create the exclusionary rule for violations of the Fourth Amendment. They could have done so. . . . The exclusionary rule is instead a judicially created rule of procedure that fails to serve the goals it seeks, and fails at a tremendous cost.

PRESIDENT'S TASK FORCE ON VICTIMS OF CRIME FINAL REPORT 24-25 (1982), *available at* http://www.ojp.gov/ovc/publications/presdntstskforcrprt/welcome.html.

[19] 631 F.3d 900 (8th Cir. 2011).

[20] *See* Brief for the United States at 1, United States v. Kramer, 631 F.3d 900 (8th Cir. 2011) (No. 10-1983).

[21] *Id.* at 4.

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.* at 5.

[26] *Id.*

subsequently arrested in the parking lot of the bar, and the victim was reunited with her family.[27]

On December 21, 2009, Kramer pleaded guilty to the charge of transportation of a minor with the intent to engage in criminal sexual activity, in violation of 18 U.S.C. § 2423(a).[28] Although Kramer admitted to the unlawful behavior, his real dispute in the courts focused on the consequences of his action: the length of his incarceration. Under the federal statutes at issue, if it was found that Kramer used a computer to commit his crimes, his sentence could be substantially increased. The definition of "computer" became a controversial focal point as the case moved through the court system.

At his sentencing hearing, Kramer argued that the evidence was inadequate to establish that his cell phone was, in fact, a computer.[29] Among Kramer's arguments was that his phone did not access the Internet.[30] The government countered by arguing that Kramer's cellular phone could act "as a calculator, [while also] storing music, digital photographs, and video . . . ."[31] The district court judge agreed with the prosecutor's position, concluding that Kramer's cellular phone was, in every important respect, indistinguishable from a traditional computer.[32] That finding allowed a "two-level" enhancement of Kramer's punishment under federal sentencing law.[33] Kramer appealed his conviction, which was affirmed on February 8, 2011, in an opinion by Judge Wollman.[34]

In reaching his decision, the judge quoted one of the modern innovators of computers at the outset of his opinion. The judge quoted Steve Wozniak, co-founder of Apple Computer, recently commenting that "[e]verything has a computer in it nowadays."[35] He posed the question at issue in the appeal of whether an ordinary cellular phone—used only to place calls and send text messages—constituted a computer.[36] He observed that the district court, relying on the definition of "computer" found in 18 U.S.C. § 1030(e)(1), enhanced Neil Kramer's sentence for transporting a minor in interstate commerce with the intent to engage in criminal sexual activity with her, a violation of 18 U.S.C. § 2423(a).[37]

---

[27] *Id.*

[28] *Id.* at 3.

[29] *Id.* at 6.

[30] *Id.* at 12.

[31] *Id.* at 10.

[32] *Id.* at 6.

[33] *Id.* at 7.

[34] United States v. Kramer, 631 F.3d 900, 900-01 (8th Cir. 2011).

[35] *Id.* at 901.

Judge Wollman noted that at trial, defendant Kramer "acknowledged that he used his cellular telephone—a Motorola Motorazr V3—to make voice calls and send text messages to the victim for a six-month period leading up to the offense."[38] At the earlier proceedings, the district court concluded that Kramer's cellular phone was a "computer" pursuant to 18 U.S.C. § 1030(e)(1).[39] The district court then "applied a two-level enhancement for its use to facilitate the offense, *see* U.S. Sentencing Guidelines Manual § 2G1.3(b)(3) (2009), and sentenced Kramer to 168 months' imprisonment."[40] Although the sentence given by the judge was "within both the original and enhanced guidelines ranges, the district court acknowledged that without the enhancement it would have sentenced Kramer to 140 months' imprisonment."[41] The judge's statement about enhancement made it clear that he was relying on the fact that the phone was a computer for purposes of increasing Kramer's punishment.

Noting an objection to the judge's ruling, Kramer argued "that application of the enhancement was procedural error because a cellular telephone, when used only to make voice calls and send text messages, cannot be a 'computer' as defined in 18 U.S.C. § 1030(e)(1)."[42] Kramer further complained that "even if a phone could be a computer, the government's evidence was insufficient to show that his phone met that definition."[43] The U.S. Sentencing Guidelines Manual § 2G1.3(b)(3) provides a two-level enhanced punishment for "the use of a computer . . . to . . .

---

[36] *Id.* at 902.
[37] *Id.* at 901.
[38] *Id.* at 901-02.
[39] *See* United States v. Kramer, 631 F.3d 900, 902 (8th Cir. 2011).
[40] *Id.* at 902.
[41] *Id.*
[42] *Id.*
[43] *Id.*

persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct . . . ."[44]

The broad definition of "computer" in criminal statute 18 U.S.C. § 1030(e)(1),[45] provides that any "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility . . . ."[46] might satisfy the statutory requirements to qualify as a computer. It is clear, however, that "an automated typewriter or typesetter, a portable hand held calculator, or other similar device" would not be included in the definition of a computer.[47]

Kramer believed that "the district court incorrectly interpreted the term 'computer' to include a 'basic cell phone'" that he used only to call and send text messages to the victim.[48] The circuit court rejected Kramer's view that the sentencing "enhancement should apply only when a device is used to access the Internet."[49] Relying on the broad language of 18 U.S.C. § 1030(e)(1), the court held that "an electronic . . . or other high speed data processing device performing logical, arithmetic, or storage functions," is a computer.[50] The court noted that "[t]his definition captures any device that makes use of a [sic] electronic data processor, examples of which are legion."[51]

Kramer argued before the trial court that the word "electronic" modifies "high speed data processing device"[52] and therefore the device must be both "electronic" and "high speed."[53] The government countered that argument by asserting that "electronic, magnetic, optical, [and] electrochemical"[54] data processing devices are, by their nature, "high speed."[55] Further, they argued that the language, "other high speed," was included by Congress "to expand the statute to cover additional types of high-speed devices that were not, or could not be, enumerated."[56] After considering both arguments, the circuit court decided not to resolve the disputed reading of the statute. It reasoned that "even if Kramer's reading of the statute is correct, a modern cellular phone can be a 'high speed' electronic device" and thus qualify a defendant for an enhanced penalty.[57] The circuit court further explained: "Indeed, modern cellular phones process data at comparable or faster rates than the desktop computers that existed when § 1030(e)(1) was enacted."[58]

---

[44] *Id.*

[45] *See* U.S. Sentencing Guidelines Manual § 2G1.3(b)(3) cmt. at 205 n.1 (2009) ("'Computer' has the meaning given that term in 18 U.S.C. § 1030(e)(1).").

[46] *Id.*

[47] *Id.*

[48] United States v. Kramer, 631 F.3d 900, 902 (8th Cir. 2011).

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] United States v. Kramer, 631 F.3d 900, 902 (8th Cir. 2011).

[54] *Id.*

[55] *Id.*

The court noted in dicta that a high speed electronic storage device could potentially include "coffeemakers, microwave ovens, watches, telephones, children's toys, MP3 players, refrigerators, heating and air-conditioning units, radios, alarm clocks, televisions, and DVD players, in addition to more traditional computers like laptops or desktop computers."[59]

It further explained that "each time an electronic processor performs any task—from powering on, to receiving keypad input, to displaying information—it performs logical, arithmetic, or storage functions. These functions are the essence of its operation."[60]

The circuit court also concluded that there was "nothing in the statutory definition that purports to exclude devices because they lack a connection to the Internet."[61] Although the court acknowledged that the term computer "does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device,"[62] it did not think Congress intended to exclude all non-Internet-enabled devices from the definition of "computer."[63]

---

[56] *Id.*

[57] *Id.* at 903 n.3.

[58] *Id.*

[59] *Id.* at 903 (quoting Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1577 (2010)) (internal quotation marks omitted).

[60] United States v. Kramer, 631 F.3d 900, 903 (8th Cir. 2011).

[61] *Id.*

[62] *Id.*

[63] *Id.*

Although the circuit court acknowledged that a "basic" cellular phone might not easily fit within the colloquial definition of "computer,"[64] the court asserted it was bound "not by the common understanding of that word, but by the specific—if broad—definition set forth in § 1030(e)(1)."[65] The court surprisingly acknowledged that "it may be that neither the Sentencing Commission nor Congress anticipated that a cellular phone would be included in that definition."[66]

At the district court hearing, "[t]he government did not, however, offer any expert testimony regarding the phone's capabilities."[67] The circuit court noted that "the materials presented to the district court were sufficient to show by a preponderance of the evidence that Kramer's phone was an 'electronic . . . or other high speed data processing device' that 'perform[ed] logical, arithmetic, or storage functions' when it was used by Kramer to call and text message the victim."[68]

From the phone's user's manual presented to the trial court by the prosecution, "the phone is powered by a '680 mAh Li-ion' battery, has '5MB' of memory, is capable of running software, makes use of a 'Graphic Accelerator' to run its color display screens, has a 'User-customizable' main menu, and comes with 'Preloaded' text messages."[69]

The user's manual "warns that the phone may include copyrighted Motorola and third-party software stored in semiconductor memories or other media."[70] Thus, these features "are sufficient to show that the phone makes use of an electronic data processor . . . [and] performs arithmetic, logical, and storage functions when the phone is used to place a call. The user's manual notes that the phone 'keeps lists of incoming and outgoing calls, even for calls that did not connect.'"[71] Furthermore, cell phones tracked "the elapsed time from the moment [the user] connect[s] to [the] service provider's network to the moment [the user] end[s] the call by pressing [the end key]."[72] The phone's counting function was a key element supporting the circuit court's finding that the phone met the requirements of the statute.[73] These capabilities all supported the district court's conclusion that the phone performed arithmetic, logical, and storage functions when Kramer used it to send text messages to the victim.[74]

---

[64] *Id.*

[65] United States v. Kramer, 631 F.3d 900, 903 (8th Cir. 2011).

[66] *Id.*

[67] *Id.* at 904.

[68] *Id.*

[69] *Id.* (internal citations omitted).

[70] United States v. Kramer, 631 F.3d 900, 904 (8th Cir. 2011) (internal quotations omitted).

[71] *Id.*

II. WHY IS THE *KRAMER* DECISION IMPORTANT FOR THE FUTURE?

A simple judicial decision defining a basic term in a statute should not raise an eyebrow given that courts perform such a function daily. The *Kramer* decision seems to fit the mold of an ordinary opinion at first glance. Upon closer examination, the case sends a subtle message of legislative responsibility for the language that it creates. The opinion curiously begins by citing one of the icons of the high technology age, one of Apple Computer's founders.[75] By starting the opinion with this acknowledgment of innovation in communications technology, one might suspect the movement of technology would play a prominent role in the opinion. Yet this was not the case. The judge paid only minor lip service to the technological ramifications of defining nearly every modern cell phone as a computer for the purpose of federal sentencing enhancement.

Using a dictionary definition approach[76] to decide the case, the court mentioned little of the long-term importance of its opinion on future criminal investigations or other matters involving emerging technology. If the clear outcome of *Kramer* dictates the use of simple statutory construction in defining "computer," then perhaps the question is settled.[77] Privacy advocates may feel there is no need for alarm. Indeed, law enforcement is no doubt content with the outcome that a defendant like Neil Kramer can be punished more severely because he used a "computer" to commit his crime. The police, after all, can be expected to use the full arsenal of weapons at their disposal to detect and prove criminal activity.[78] After all, Kramer committed what many feel is the most serious crime of all—a sexual offense against a minor.[79] Surely Congress could not be faulted for trying to achieve the goal of severely punishing such offenders. Assuming Congress intended such a broad definition of a computer as the court in *Kramer* suggests, what does *Kramer*'s holding mean for other courts facing similar questions involving emerging technologies?

---

[72] *Id.*

[73] *Id.* at 905.

[74] *Id.*

[75] United States v. Kramer, 631 F.3d 900, 901 (8th Cir. 2011).

[76] *See* THE NEW OXFORD AMERICAN DICTIONARY 277 (2d ed. 2005) (defining "central processing unit" as "the part of a computer in which operations are controlled and executed").

[77] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1577 (2010) ("Just think of the common household items that include microchips and electronic storage devices, and thus will satisfy the statutory definition of 'computer.'").

Think about the type of evolving technologies that routinely seize and store all kinds of information that some may consider private. Every time a vehicle goes through a toll booth the tag is recorded and linked to whatever sensitive information is attached to that registered vehicle's owner.[80] Similarly, speed and red light photo cameras record images[81] of a driver and his or her passengers while noting the time of travel.[82] Gasoline purchase records document how much fuel is in a vehicle and the location of purchase with startling accuracy.

---

[78] Thomas K. Clancy, noted this flexibility in law enforcement:

> Crime has changed, as have the means of law enforcement, and it would therefore be naive to assume that those actions a constable could take in an English or American village three centuries ago should necessarily govern what we, as a society, now regard as proper. Thus, the Court has sometimes asserted that the Amendment's "prohibition against 'unreasonable searches and seizures' must be interpreted 'in light of contemporary norms and conditions.'"

Thomas K. Clancy, *What Constitutes an "Arrest" Within the Meaning of the Fourth Amendment?*, 48 VILL. L. REV. 129, 184 (2003) (footnote omitted) (quoting Steagald v. United States, 451 U.S. 204, 217 n.10 (1981)) (internal quotation marks omitted).

[79] Law enforcement obviously needs data in order to investigate and prosecute crime. High technology has proven particularly useful in the prosecution of offenders engaged in child pornography. *See* Jason Krause, *Can Anyone Stop Internet Porn?: Courts Have Shot Down Laws Protecting Kids from Obscenity Online. Is Cyberspace Suited for a Virtual Privacy Wrapper?*, 88 A.B.A. J., Sept. 2002, at 56.

[80] Public use of intrusive video technology is growing. *See* M.J. Zuckerman, *Chances Are, Somebody's Watching You*, USA TODAY, Nov. 30, 2000, at 01.A (describing a forty million dollar surveillance center using 110 remote control cameras in the suburbs of Washington).

[81] New forms of surveillance technology that actually record facial images and compare features to other persons located in computer databases have been increasingly used by law enforcement. *See* Christopher S. Milligan, Note, *Facial*

When a customer shops for groceries, the store records the customer's purchases to identify preferences. These records of tastes and prior choices are recorded to allow the merchant to offer a coupon to purchase your favorite tissue paper days before it runs out. Cellular phones are capable of locating individuals almost anywhere in the world with startling accuracy. All of these intrusions are given little thought because of the conveniences the technology brings to our lives. Instant coupons, weekly special values, discounts for future purchases, and other inducements make us surrender our e-mail addresses to take advantage of these benefits. In short, citizens love the ease and comfort these technologies afford.

Law enforcement has benefited greatly from the accuracy of record keeping that the computer era has provided. Little thought is given to where this information "lives" or is stored when it is waiting to be reviewed or retrieved.[83] It is usually unclear who

---

Recognition Technology, Video Surveillance, and Privacy, 9 S. CAL. INTERDISC. L.J. 295, 303-08 (1999) (describing digital and biometrics technology).

[82] Consider, as an example of intrusion, the use of red light cameras, which has emerged over the last decade. Currently, the surveillance method is so common that we are no longer surprised by the mailed notices, capturing our vehicle and often a passenger, the time of violation, and our exact location at a camera-equipped intersection. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). One federal court had this comment about the law:

> The passage of the Patriot Act altered and to some degree muddied the landscape. In October 2001, Congress amended FISA [Foreign Surveillance Intelligence Act] to change "the purpose" language . . . . It also added a provision allowing "Federal officers who conduct electronic surveillance to acquire foreign intelligence information" to "consult with Federal law enforcement officers to coordinate efforts to investigate or protect against" attack or other grave hostile acts, sabotage or international terrorism, or clandestine intelligence activities, by foreign powers or their agents.

In re Sealed Case Nos. 02-001, 02-002, 310 F.3d 717, 728-29 (FISA Ct. Rev. 2002).

[83] If there is any doubt that the government continues to construe *Smith v. Maryland*, 442 U.S. 735 (1979), with any less than the broadest possible scope, the testimony of Deputy Associate Attorney General Kevin DiGregory during a congressional hearing on government surveillance issues is instructive. DiGregory said:

> [T]he Supreme Court held, in Maryland versus Smith [sic], I believe, in 1979, that there was no reasonable expectation of privacy in numbers dialed by a telephone, because essentially, when someone turns over information to a

has permission to review this information. These concerns have raised little alarm so long as a better "smart phone" is on the way soon.[84]

One might suggest that in many of the concerns I raise the user of the technology knowingly and willingly exposes their information to third parties—in the cases of seized photographic images, they may not be considered private at all.[85] Furthermore, since much of the information that I have complained about is not seized by government officials, it is not private at all or even subject to Fourth Amendment review. Even when the Fourth Amendment is implicated, courts sometimes struggle with where the line of protection should be drawn when new technologies are involved.[86] Thus, we may have surrendered our personal

---

> third party, like the telephone company, they should not have either a subjective or an objective reasonable expectation of privacy in that information.

Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary, 106th Cong. (2000) (emphasis added) (statement of Kevin V. DiGregory, Deputy Assoc. Att'y Gen., U.S. Dep't of Justice).

[84] All eyes have been trained on News Corp. in recent weeks, following allegations that the now-defunct *News of the World* hacked the phones of more than 4000 politicians, crime victims, and celebrities:

> [T]he art of getting people to inadvertently divulge information through seemingly innocuous questions—is one way, and it's as simple as going on a website and tricking a system or individual. For example, Christopher Soghoian, a fellow at the Center for Applied Cypersecurity [sic] Research, in a quick email shared a website called phonegangster.com. The website can send visitors directly to a voicemail account, where they can insert a pass code by spoofing a phone number.

Lyneka Litle, *Murdoch Scandal Fallout: Consumers Make Cell Phone Hacking Easy*, ABC NEWS (July 22, 2011), http://abcnews.go.com/Business/murdoch-scandal-fallout-consumers-make-cell-phone-hacking/story?id=14128470&singlePage=true.

[85] The storing of visual images, in general, raises many concerns in society. "Video-surveillance cameras quietly scan many workplaces. Neighborhood retailers now stock hardware that used to be the stuff of spy novels." Richard Lacayo, Tom Curry, Thomas McCarrol & Dennis Wyss, *Assaulting Our Privacy: Nowhere to Hide*, TIME, Nov. 11, 1991, at 34.

[86] Tracey Maclin, Katz, Kyllo, *and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51-52 (2002) ("Advances in science and technology recurrently exert pressure on the scope and meaning of the Fourth Amendment, but the privacy and security protected by the Fourth Amendment should not depend on innovations and technology. . . . During the Framers' era, the home was the focal point of privacy and personal security." (footnote omitted)). "When the American Republic was founded, the framers established a libertarian equilibrium

information without much thought as to who might retrieve it or if we can limit its use. We have simply allowed it to be sent to the winds, incapable of ever controlling it again.[87] With the exception of some medical[88] and financial data,[89] very little statutory protection is provided for much of the information routinely communicated over our "computer phones." Has this truly been a willing choice, or have we simply been enchanted by the science of communication?[90] Perhaps it does not matter anymore. The average citizen has lost so much control over their personal information that it may be impossible to reverse the trend.[91] Perhaps the benefits of technology are so great we simply do not care about how our privacy has been diminished.[92] Perhaps the

---

among the competing values of privacy, disclosure and surveillance." ALAN F. WESTIN, PRIVACY AND FREEDOM 67 (1967).

[87] One scholar has gone so far as to suggest that "[i]n this era of rapid technological change, the freedom to be unnoticed in public, and its associated benefits, will disappear unless a right to public anonymity is recognized and enforced." Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 217, 314-15 (2002) (arguing that the Fourth Amendment should be construed to recognize a right to public anonymity as a part of privacy expectations because "government surveillance of our innocent public activities that are not meant for public consumption is neither expected nor to be condoned").

[88] Tracey Maclin, *Let Sleeping Dogs Lie: Why the Supreme Court Should Leave Fourth Amendment History Unabridged*, 82 B.U. L. REV. 895, 933-34 (2002). The Supreme Court rejected a challenge to a New York central computer databank containing the names and addresses of all persons obtaining drugs by prescription.

[89] United States v. Miller, 425 U.S. 435, 442-43 (1976) (citing United States v. White, 401 U.S. 745, 751-52 (1971)) (finding no reasonable expectation of privacy in financial information contained at the defendant's bank because a "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the [g]overnment"); FRANK J. DONNER, THE AGE OF SURVEILLANCE 7 (1980).

[90] *See* James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 425 n.386 (2002) ("As society has evolved and our lives have become more mobile, as we spend more and more of our waking hours away from home, there may be even more reason to prize our right to preserve secrecy outside dwellings and to be concerned with novel perils generated by scientific and technological progress.").

[91] "Repeated invasions by credit bureaus, employers, and the like can lead persons to discount most expectations as unreasonable; individual fears of a loss of privacy then become self-fulfilling prophecies. In particular, the government can through its actions redefine popular expectations so as to undermine constitutional rights." Comment, *Legitimate Expectations of Privacy Against Unreasonable Searches and the "Automatic Standing Rule,"* 94 HARV. L. REV. 196, 203 (1980).

[92] The value of personal privacy has been a concept that many thinkers have pondered for well over a century. One particularly longstanding comment of privacy reminds us that "[p]olitical, social, and economic changes entail the recognition of new

Kramer court's casual approach to controlling emerging technology reflects our casual attitude toward the protection of privacy.[93]

CONCLUSION

Maybe there is no Big Brother[94] to worry about after all, only Little Brother! If we like that law enforcement is having an easier time prosecuting crime because of the computer, there is no need to be alarmed. If we want our local grocer to remind us we are running out of coffee, we are happy for them to evaluate our kitchen closet.[95] If we want our computer to remember the web site we visited a week ago to get a recipe, perhaps we do not mind if our internet service provider sells our information to a cooking school.[96] In an age when fear of terrorism dominates both the need

---

rights, and the common law, in its eternal youth, grows to meet the demands of society. . . . [T]he right to be let alone . . . has grown to comprise every form of possession—intangible, as well as tangible." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1891).

[93] The challenge for the *Kramer* court was to take seriously the very real threat posed to societal privacy by what appears to many to be a routine case. Such decisions also pose a danger of courts being too casual with their role as protector of individual liberty. One insightful commentator has noted that "technological advances pose the challenges that always beset the constitutional enterprise—those involved with trying to create fixed rules, or at least a workable rule of law, for a changing world." Susan Bandes, *Power, Privacy and Thermal Imaging*, 86 MINN. L. REV. 1379, 1383 (2002).

[94] M. ETHAN KATSH, LAW IN A DIGITAL WORLD 227-28 (1995) ("In Orwell's society, there was no right of privacy or expectation of privacy. In our society, privacy is highly valued and some legal rights of privacy do exist. Yet privacy, in the sense of being able to control information about oneself, is also an eroding condition." (footnote omitted)).

[95] Whalen v. Roe, 429 U.S. 589, 605 (1977) ("We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. . . . The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.").

[96] An important aspect of electronic searches is their potential scope. They are not merely limited to information or historical facts, but also permit access to discovering future events. As one commentator explained:

> The conventional search is limited to a designated thing in being—one of a finite number of things to be found in the place where the search is to be conducted, and ordinarily discoverable in a single brief visit. On the other hand, electronic surveillance is a quest for something which may happen in the future. Its effectiveness normally depends upon a protracted period of lying-in-wait. For however long that may be, the lives and thoughts of many people—not merely the immediate target but all who chance to wander into the web—are exposed to an unknown and undiscriminating intruder. Such a

and the use of intrusive technology,[97] we are likely to discount the very protections envisioned by our Founding Fathers in the Bill of Rights. Again, we are often reminded that the desire to be secure should always dominate our need to choose more privacy when intrusion becomes both quick and easy.

Perhaps George Orwell was correct about the final outcome of all this technology when he said, "Forty years it had taken him to learn . . . . O cruel, needless misunderstanding! . . . But it was all right, everything was all right, the struggle was finished. He had won the victory over himself. He loved Big Brother."[98] Perhaps we

---

> search has no channel and is certain to be far more pervasive and intrusive than a properly conducted search for a specific, tangible object at a defined location.

Ralph S. Spritzer, *Electronic Surveillance by Leave of the Magistrate: The Case in Opposition*, 118 U. PA. L. REV. 169, 189 (1969).

[97] David Hardin, Note, *The Fuss over Two Small Words: The Unconstitutionality of the USA PATRIOT Act Amendments to FISA Under the Fourth Amendment*, 71 GEO. WASH. L. REV. 291, 345 (2003) ("Although the conflicting interests involved are compelling, the paramount function of national security is to vigilantly protect the ideals embodied by the very same Amendment that the standard violates. Those ideals cannot be whittled away in today's desire to defend the very same values that provide for our security.").

[98] ORWELL, *supra* note 2. In a recent Supreme Court oral argument regarding whether it was constitutional for the government to track anyone it choose by attaching a Global Positioning Satellite device on their vehicle (GPS), the following exchange occurred between the government attorney and Chief Justice John Roberts, reflecting the potential consequences of the government's willingness to use technology in law enforcement:

> CHIEF JUSTICE ROBERTS: You think there would also not be a search if you put a GPS device on all of our cars, monitored our movements for a month? You think you're entitled to do that under your theory?
>
> MR. DREEBEN: The justices of this Court?
>
> CHIEF JUSTICE ROBERTS: Yes. (Laughter.)
>
> MR. DREEBEN: Under our theory and under this Court's cases, the justices of this Court when driving on public roadways have no greater expectation
>
> CHIEF JUSTICE ROBERTS: So your answer is yes, you could tomorrow decide that you put a GPS device on every one of our cars, follow us for a month; no problem under the Constitution?

should think about what we are giving up and not be so quick to fall in love.[99]

> MR. DREEBEN: Well, equally, Mr. Chief Justice, if the FBI wanted to it could put its team of surveillance agents around the clock on any individual and follow that individual's movements as they went around on the public streets and they would thereby gather . . . .

Transcript of Oral Argument at 9-10, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10–1259).

[99] It has been argued that a "good society must have its hiding places—its protected crannies for the soul. Under the pitiless eye of safety the soul will wither." Charles A. Reich, *Police Questioning of Law Abiding Citizens*, 75 YALE L.J. 1161, 1172 (1965).

A UNIFIED THEORY FOR SEIZURES OF THE PERSON

Ronald Bacigal[*]

INTRODUCTION....................915
I. THE EVOLUTION OF *TERRY* AND ITS PROGENY....................916
II. THE QUEST FOR UNITY....................923
III. A PROPOSAL FOR UNIFICATION....................927
IV. A ROLE FOR *MENDENHALL*?....................934
CONCLUSION: THE PROPOSED UNIFIED THEORY....................936

INTRODUCTION

Perhaps there is something about the final stages of their careers that causes people to resolve conflicts by reconciling the seemingly irreconcilable. Albert Einstein spent the last days of his career searching for a unified field theory that would eliminate the contradictory laws governing relativity and quantum mechanics.[1] Stephen Hawking has taken up this quest which has been renamed a search for the Theory of Everything.[2]

On a "slightly" more modest level, I find the later stages of my career drawing me toward formulating a unified theory governing seizures of the person. The challenge is to blend three different tests the Supreme Court has applied when defining a Fourth Amendment seizure. These tests were articulated, over a period of eleven years, in *United States v. Mendenhall*,[3] *Brower v. County of Inyo*,[4] and *California v. Hodari D.*[5] Before addressing those cases, however, we must begin at the beginning with an examination of *Terry v. Ohio.*[6] Not to belabor the references to physics, but *Terry* is the big bang that starts the modern world of variable levels of seizures of the person.

---

[*] Professor of Criminal Law, Criminal Procedure & Evidence, University of Richmond School of Law. B.S., Concord University; LL.B., Washington & Lee University.

[1] James R. Hackney, Jr., *The "End" of: Science, Philosophy, and Legal Theory*, 57 U. Miami L. Rev. 629, 632 (2003) ("Einstein would end his career in science searching for a "unified field theory" that would serve as the type of totalizing theory of the physical world that Newton had been thought to have constructed. It was a failed effort.").

[2] *See* STEPHEN HAWKING & LEONARD MLODINOW, THE GRAND DESIGN (2010). A Theory of Everything (TOE) is a putative theory of theoretical physics that fully explains and links together all known physical phenomena, and predicts the outcome of *any* experiment that could be carried out *in principle*. *See id.*

I. THE EVOLUTION OF *TERRY* AND ITS PROGENY

All students of the Fourth Amendment can recite the facts of *Terry*:

> While on patrol, Officer McFadden observed the action of three men he suspected of "casing a job, a stickup." He approached the three men, identified himself as a police officer and asked for their names. When the men "mumbled something" in response to his inquiries, Officer McFadden grabbed petitioner Terry, spun him around so that they were facing the other two, with Terry between McFadden and the others, and patted down the outside of his clothing. In the left breast pocket of Terry's overcoat Officer McFadden felt a pistol.[7]

What is often overlooked when discussing *Terry* is that the opinion actually said very little about defining the initial seizure of the person. This oversight is not the Court's fault because it cautioned that "[t]he crux of this case, however, is not the propriety of Officer McFadden's taking steps to investigate petitioner's suspicious behavior, but rather, whether there was justification for McFadden's invasion of Terry's personal security by searching him for weapons in the course of that investigation."[8]

---

[3] 446 U.S. 544 (1980).

[4] 489 U.S. 593 (1989).

[5] 499 U.S. 621 (1991).

[6] 392 U.S. 1 (1968).

[7] *Id.* at 4-7.

[8] *Id.* at 23. Less there be any doubt the Court was dodging the constitutionality of the initial stop, footnote 16 went on to explain:

> We thus decide nothing today concerning the constitutional propriety of an investigative "seizure" upon less than probable cause for purposes of "detention" and/or interrogation. . . . We cannot tell with any certainty upon this record whether any such "seizure" took place here prior to Officer McFadden's initiation of physical contact for purposes of searching Terry for

The *Terry* opinion ignored the officer's initial approach to the suspects—the stop half of stop-and-frisk—and instead focused on the frisk part that occurred when the officer spun the defendant around and patted his outer clothing. The fundamental issue in *Terry* was not whether the government established some physical control of the person—that was undisputed. The issue was the degree of control required for a Fourth Amendment seizure.[9] Prior to *Terry*, the Amendment had covered only full custodial arrests,[10] and Terry had not been arrested when he was patted down. The significance of *Terry* was to shatter the monolithic view that an arrest was the only type of seizure that counted.[11] *Terry* adopted the approach that we now take for granted—that the Fourth Amendment is flexible enough to take account of different levels of seizures, which require different levels of justifications. Thus, the frisk in *Terry* constituted a lesser seizure than an arrest, which accordingly could be justified by a lower standard of reasonable suspicion, instead of probable cause.

Following *Terry*, a number of cases touched on the initial seizure of a citizen, but it was not until 1980 in *United States v. Mendenhall*, that the Supreme Court definitively addressed the issue it had sidestepped in *Terry*—the stop half of stop-and-frisk.[12] There was no frisk in *Mendenhall*, which was the first of the airport encounter cases involving DEA agents approaching a suspected drug currier in an airport concourse in order to ask her questions—the stop and interrogate situation that *Terry* ignored.[13] The *Mendenhall* Court now focused on the initial encounter

---

> weapons, and we thus may assume that up to that point no intrusion upon constitutionally protected rights had occurred.

Id. at 19 n.16.

[9] *Id.* at 16-31.

[10] *Id.* at 19 (rejecting "the notions that the Fourth Amendment does not come into play at all as a limitation upon police conduct if the officers stop short of something called a 'technical arrest'").

[11] *Id.* at 16 ("It is quite plain that the Fourth Amendment governs 'seizures' of the person which do not eventuate in a trip to the station house and prosecution for crime—'arrests' in traditional terminology.").

[12] United States v. Mendenhall, 446 U.S. 544, 552-53 (1980) ("What was not determined in [*Terry*], however, was that a seizure had taken place before the officer physically restrained Terry for purposes of searching his person for weapons.").

[13] *See id.*; *see also* United States v. Place, 462 U.S. 696 (1983); Florida v. Royer, 460 U.S. 491 (1983).

between police and citizen, and whether that interaction constituted a Fourth Amendment seizure or a wholly voluntary encounter beyond the Amendment's coverage. Unlike Officer McFadden in *Terry*, the DEA agents in *Mendenhall* were not physically spinning the suspect around and patting her down; rather, they were asking for, or demanding, identification and that she submit to interrogation.[14] Based on these facts, the Court formulated its initial definition of a seizure: "[A] person has been 'seized' within the meaning of the Fourth Amendment only if, in view of all of the circumstances surrounding the incident, a reasonable person would have believed that he was not free to leave."[15] The Court concluded that the defendant in *Mendenhall* had not been seized when first approached in the concourse, nor when she voluntarily went to another room and consented to a strip search.[16]

Three years later in *Florida v. Royer*, the *Mendenhall* test was applied to a similar airport encounter between the suspect and the police, but with drastically different results.[17] Now, not only had the defendant been seized, he had been arrested,[18] which required full probable cause, [19] not the lower standard of reasonable suspicion established in *Terry*. *Royer* also fleshed out *Mendenhall's* test for seizures by listing the factors that are relevant in determining which of three possibilities had occurred: (1) a wholly voluntary encounter—not covered by the Amendment; (2) a limited detention—covered, but justified by a lower standard of reasonable suspicion; or (3) a full custodial arrest necessitating compliance with all Fourth Amendment requirements.[20]

---

[14] *Compare Terry*, 392 U.S. at 7 ("Officer McFadden grabbed petitioner Terry, spun him around so that they were facing the other two [men], with Terry between McFadden and the others, and patted down the outside of his clothing."), *with Mendenhall*, 446 U.S. at 548 ("Agent Anderson asked the respondent if she would accompany him to the airport DEA office for further questions. She did so, although the record does not indicate a verbal response to the request.").

[15] *Mendenhall*, 446 U.S. at 554 (citation omitted).

[16] *Id.* at 557-60.

[17] Florida v. Royer, 460 U.S. 491 (1983).

[18] *Id.* at 494-95.

[19] *Id.* at 507 ("We agree . . . that probable cause to arrest Royer did not exist at the time he consented to the search of his luggage.").

[20] *Id.* at 497-501.

Even after *Royer*'s helpful categorization of varying degrees of encounters between police and citizens, problems remained with *Mendenhall*'s reasonable perception test, both in theory and in application. The first question that arose was whether *Mendenhall*'s reasonable perceptions standard was a supplement to, or a substitute for, *Terry*'s emphasis on the corporeal restraint that occurred when the defendant was frisked. In other words, if there is a conflict between reality and perception, which factor is controlling? The question posed is the Fourth Amendment's variation on a classic query for beginning students of epistemology—if a tree falls in the forest and no one hears it, has there still been a sound? In the Fourth Amendment context, the riddle arises in a situation where police officers surround a suspect's dwelling to ensure that he does not depart the premises, but the suspect remains unaware of the officers' presence.[21]

This hypothetical situation demonstrates that at least a partial restriction of the defendant's liberty[22] may occur without his awareness of that fact, just as a clandestine search of the defendant's property, known as a "black bag job," may occur without his knowledge.[23] If *Mendenhall*'s focus upon a person's perceptions trumps any actual but secret restraint, the definitions of searches of property and seizures of a person are strangely juxtaposed. A covert governmental intrusion upon privacy triggers Fourth Amendment protections, while a covert intrusion upon an individual's liberty or freedom of movement lacks constitutional significance until it is accompanied by perception of the intrusion.

The other half of the *Terry*/*Mendenhall* paradox was whether the Fourth Amendment applied when there was the perception, but not the reality, of restraint—that is, someone believes he heard a falling tree, but in fact no tree fell. For example, consider the "mistaken motorist" hypothetical, where a motorist observes an officer in a trailing police car activate the car's siren and flashing lights. As the motorist pulls over to the side of the road, believing that the police have ordered him to stop, the police pass him by in order to stop a vehicle further down the highway.[24] The motorist's mistaken, but perfectly reasonable, perception of government imposed restraint satisfies the *Mendenhall* test for a seizure of the person, even though the police never exercised any control over the motorist's freedom of movement.[25]

---

[21] The hypothetical is based on the facts of *State v. White*, 838 P.2d 605 (Or. Ct. App. 1992), where police surrounded the defendant's dwelling and the defendant complied with the order that he exit the dwelling. The majority and concurring opinions differed as to whether the defendant had been seized while still inside the house, or not until he had exited the dwelling. *Compare id.* at 609-12 (Durham, J., concurring), *with id.* at 608 (majority opinion).

[22] Although the suspect remains free to move about inside his residence, he is not free to depart. *Cf.* INS v. Delgado, 466 U.S. 210, 218 (1984) (holding that no seizures occurred by stationing guards at exits because the guards' purpose was not to prevent exit, but to ensure that all persons were questioned).

[23] *See* Lloyd L. Weinreb, *Generalities of the Fourth Amendment*, 42 U. CHI. L. REV. 47, 53 (1974) ("A person's home is a place that he expects will not be invaded whether he is present or absent.").

This aspect of the riddle—can perception outweigh reality—was partially resolved in *Brower v. County of Inyo*, where the Court answered a variation on the mistaken motorist hypothetical by supplementing the *Mendenhall* test for seizures with a second test.[26] *Brower* held that the Fourth Amendment does not encompass "the accidental effects of otherwise lawful government conduct,"[27] and that no seizure occurs unless the police utilize "means intentionally applied"[28] to bring about the seizure.

The actual holding of *Brower* is not surprising—a motorist eluding pursuing police was seized at the point that he was stopped by a police roadblock erected for the very purpose of stopping him.[29] The controversial aspect of *Brower* arose from the Court's holding that no seizure occurred during the twenty-mile chase leading up to the roadblock, and the Court's agreement with the Sixth Circuit that no seizure occurred in *Galas v. McKee*, a case in which a fleeing suspect lost control of his vehicle and crashed during a high-speed chase with the police. [30] The Sixth

---

[24] *See* State v. Indvik, 382 N.W.2d 623, 627 (N.D. 1986) ("There may be several motorists in the vicinity of an officer when he uses his flashing red lights. To constitute a stop by the use of flashing red lights, the officer must have the intent to stop the specific motorist and the motorist must be cognizant of the officer's presence.").

[25] In the hypothetical, there is *self-imposed* restraint but only an erroneous perception of *government* restraint.

[26] Brower v. County of Inyo, 489 U.S. 593 (1989).

[27] *Id.* at 596.

[28] *Id.* at 597 (emphasis omitted).

[29] *Id.* at 599 (Authorities "sought to stop Brower by means of a roadblock and succeeded in doing so. That is enough to constitute a 'seizure' within the meaning of the Fourth Amendment.").

[30] *Id.* at 595; *see also* Galas v. McKee, 801 F.2d 200, 203 (6th Cir. 1986).

Circuit explained in *Galas* that no seizure occurred because the "restraint on plaintiff's freedom to leave [the crash] . . . was not accomplished by the show of authority but occurred as a result of plaintiff's decision to disregard it."[31] The chases in both *Galas* and *Brower* obviously satisfied the *Mendenhall* test because reasonably prudent people certainly understand they are not free to leave when a pursuing police car activates sirens and flashing lights. *Brower*, however, taught that the reasonable perceptions of the *Mendenhall* test are not enough to trigger Fourth Amendment protections.

After *Brower*, there were now two tests for defining a seizure, but they were not inherently inconsistent because both *Brower* and *Mendenhall* can be satisfied by one set of facts, e.g., the very facts of *Brower*. But there are other situations where the two tests may conflict. For example, suppose a citizen thinks he is free to depart from what he perceives to be a wholly voluntary and cordial encounter with police—"Lovely day, isn't it officers? Who do you think will win the Super Bowl?" But, in fact, this citizen is not free to leave because the police secretly have decided they will stop him should he try to depart. The officers' intent satisfies *Brower*, but *Mendenhall*'s requirement for a perception of restraint is absent.

Another problem in reconciling *Mendenhall* and *Brower* is that although *Brower*'s language regarding police intent eliminated accidental, or rather unintended, seizures from Fourth Amendment coverage, it did not establish the point at which an *intended* seizure becomes an accomplished seizure. If an officer turns on a police car's siren and flashing lights with the intent to seize a motorist, does a seizure occur when the siren and lights are activated, where the intent to seize is present and also perceived by the suspect, or only when the motorist acquiesces to this show of authority by stopping his vehicle?[32]

---

[31] *Galas*, 801 F.2d at 203.

[32] Justice Stevens posed another wrinkle to this hypothetical:

> [T]here will be a period of time during which the citizen's liberty has been restrained, but he or she has not yet completely submitted to the show of force. A motorist pulled over by a highway patrol car cannot come to an immediate stop, even if the motorist intends to obey the patrol car's signal. If an officer decides to make the kind of random stop forbidden by [*Delaware v. Prouse*, 440 U.S. 648 (1979)], and, after flashing his lights, but before the

The Court answered this question in *California v. Hodari D.* by announcing a third test for defining a seizure of the person—police intent to restrain a defendant lacks constitutional significance until the defendant is successfully apprehended.[33] Thus, *Hodari D.* did for attempted seizures what *Brower* had done for accidental seizures. Attempted seizures were placed beyond the coverage of the Fourth Amendment because a seizure occurs only when the government successfully controls the citizen, either by corporeal restraint or by obtaining his submission to a show of authority.[34]

Hodari D., like *Brower*, involved police pursuit of a fleeing suspect, this time on foot rather than by automobile. Prior to being tackled by a police officer—an undisputed seizure—the fleeing suspect discarded crack cocaine, which the police subsequently retrieved.[35] The issue was whether the crack cocaine should be suppressed as the fruit of an illegal seizure—the chase—or whether the crack cocaine was discarded prior to what could be deemed to be the only seizure that occurred—the tackling of the suspect.[36] The California courts found that a seizure had occurred during the chase itself because they applied the two existing tests to the facts of *Hodari D.*.[37] The police clearly intended to seize the defendant—satisfying the *Brower* test—and a reasonably prudent person would perceive he lacked the freedom to leave—satisfying the *Mendenhall* test—even though he still possessed the physical ability to flee.[38] But to the United States Supreme Court, neither the reasonable perceptions test of *Mendenhall*, nor the intentional means test of *Brower* were enough to constitute a seizure until police completely eliminated the suspect's physical ability to escape.[39] *Mendenhall* and *Brower*

> vehicle comes to a complete stop, sees that the license plate has expired, can he justify his action on the ground that the seizure became lawful after it was initiated but before it was completed?

California v. Hodari D., 499 U.S. 621, 645 (1991) (Stevens, J., dissenting).

[33] *Id.* at 629.

[34] *Id.* ("In sum, assuming that [Officer] Pertoso's pursuit in the present case constituted a 'show of authority' enjoining Hodari to halt, since Hodari did not comply with that injunction he was not seized until he was tackled.").

[35] *Id.* at 623.

[36] *Id.* at 624.

[37] *Id.*

[38] *See id.* at 625-26.

[39] *See id.* at 627-28.

were necessary, but not sufficient, predicates because the Court now explained that so long as the suspect was eluding the police, there was only an attempted seizure, which is not covered by the Fourth Amendment.[40]

With the decision in *Hodari D.*, the Court completed an eleven-year process of fashioning three tests for a seizure of the person. In the twenty years since *Hodari D.*, the Court has either dealt with each of the three tests in isolation, or has addressed cases where there was little question that all three tests were met. The Court, however, has said little about the relationship and possible conflict between these tests. Must all three tests be satisfied in all cases? Are two out of three close enough for government work? Or can any of the three stand alone and be sufficient in the right case? Somehow, *Terry*'s initial consideration of seizures evolved into this puzzling patchwork of three tests that are sometimes complementary and sometimes inconsistent.

II. THE QUEST FOR UNITY

Within the legal universe of the Fourth Amendment, lawyers can follow the lead of Einstein, Hawking, and other physicists in searching for a unified theory. At first blush, it appears that the physicists have an advantage over lawyers because physicists need only reconcile two conflicting principles: quantum mechanics and relativity. In contrast, the law must reconcile the three theories set forth in *Mendenhall*, *Brower*, and *Hodari D.* Yet, in the end, the physicists may have the tougher task because they are in uncharted territory, while we lawyers have the benefit of a prototype. In contrast to the multiple definitions of seizures of a person, the Court has provided a more unified theory of Fourth Amendment searches.

In his concurring opinion in *Katz v. United States*, Justice Harlan formulated a single definition of Fourth Amendment searches subsequently adopted by the full Court.[41] Once the defendant subjectively desires privacy, a search occurs when the government intrudes upon an expectation of privacy "that society is prepared to recognize as 'reasonable.'"[42] *Katz* announced that the Amendment "protects people, not places,"[43] and discarded prior definitions of a search that had focused on a factual requirement for a physical trespass.[44] In place of this factual predicate, *Katz* launched an inquiry into a broad societal view of expectations of privacy.[45]

---

[40] *Id.*

[41] 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

What makes *Katz* a useful prototype for defining the coverage of the Fourth Amendment is the fundamental difference between *Mendenhall*'s limited focus on a reasonably prudent person's perceptions of freedom to leave—a factual inquiry—versus *Katz*'s expansive focus on society's recognition of reasonable expectations of privacy. The *Mendenhall* approach is descriptive of current perceptions, while the *Katz* approach is proscriptive. *Mendenhall* tells us what we currently expect, while *Katz* tells us what we have a right to expect—"what we should demand of government."[46]

Consider how the two distinct approaches would apply to this hypothetical: As part of an effort to stem a rising tide of underwear bombers boarding planes, the government announces a new program of strip-searching all passengers. Once that program is in place, no reasonable person could expect privacy at an airport security checkpoint. But under *Katz*, the issue is whether society will tolerate those strip searches.

Katz's unified approach to searches means that all government intrusions upon privacy must be measured against but a single standard—society's reasonable expectations of privacy.[47] Given this unified theory of searches, we are left to wonder why the seizure of a person involves three separate inquiries: a reasonably prudent person's perceptions; the actual defendant being restrained or submitting to a show of authority; and the government's intent to seize. Conspicuously missing from the three tests is any mention of society's view of what constitutes a seizure. The language of the Fourth Amendment, which equally prohibits unreasonable searches and seizure of "persons, houses, papers, and effects,"[48] does not support this drastic distinction between seizures of the person and searches of a person's property.

---

[42] *Id.* at 361.

[43] *Id.* at 351.

[44] The Court stated:

> Thus, although a closely divided Court supposed in *Olmstead* [*v. United States*, 277 U.S. 438 (1928)] that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested. . . . [O]nce it is recognized that the Fourth Amendment protects people – and not simply 'areas' – against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.

Katz, 389 U.S. at 353.

[45] *Id.* at 361.

[46] Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974).

The seminal decisions defining searches and seizures, *Katz* and *Terry*, also fail to support the distinction drawn by the current Court. Prior to *Katz*, the Court had held that physical trespass to the defendant's property was a necessary factual predicate for the triggering of the Amendment's coverage of governmental searches.[49] When *Katz* shifted the Amendment's focus from property rights to the fundamental right of privacy, the requirement for a physical trespass was discarded. Despite warnings that "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy,'"[50] post-*Katz* litigation has centered on the privacy issue and the Court's need to determine which privacy values are recognized by society as "justifiable" or "legitimate" and, therefore, protected by the Amendment. Because justifiable expectations of privacy may differ from expectations currently held by "reasonable" members of society, those current expectations have been supplemented by the Court's examination of history,[51] property rights,[52] natural law,[53] and utilitarian balancing.[54]

---

[47] While a search involves privacy considerations, the Fourth Amendment also protects property interests even when privacy or liberty interests are not involved. *See* Soldal v. Cook County, 506 U.S. 56, 58 (1992) (police seized and removed, without entering, the plaintiff's mobile home during an unlawful eviction).

[48] U.S. CONST. amend. IV.

[49] *See supra* note 40 and accompanying text.

[50] *Katz*, 389 U.S. at 350.

[51] *See* United States v. Watson, 423 U.S. 411, 415-16 & n.4 (1976).

[52] *See* Rakas v. Illinois, 439 U.S. 128, 143 & n.12 ("Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.").

When Fourth Amendment analysis turns from searches of property to seizures of the person, the focal point of judicial scrutiny shifts from privacy interests to the citizen's fundamental interests in liberty[55] and freedom of movement.[56] This change in focus merely presents a different context in which the Court might be called upon to identify those societal values that the Fourth Amendment recognizes as legitimate or justifiable. In fact, because concepts of privacy and liberty often overlap, they can be seen as facets of the Amendment's overarching concern with protecting personal autonomy, what *Olmstead* referred to as "the right to be let alone . . . the right most valued by civilized men." [57] Thus, the methodology utilized to identify legitimate privacy expectations would seem to apply equally to determinations of legitimate liberty expectations.[58] We are left to wonder why the seizure cases are not following *Katz* in asking whether the government action intruded on an expectation of liberty that society is prepared to recognize as reasonable.

Katz and *Terry*, decided within a year of one another, also share a common characteristic of expanding Fourth Amendment protections beyond historical precedents. Pre-*Terry* analysis had equated seizures of a person with common law arrests. Thus, the Court in *Terry* was asked to make an all-or-nothing determination: either there was an arrest, requiring full compliance with the Fourth Amendment, or there was no arrest and the Amendment was inapplicable. Just as physical trespass had been essential to pre-*Katz* searches, arrest had been a necessary linchpin for pre-*Terry* seizures of the person.[59] *Terry*, however,

---

[53] *See generally* Warden v. Hayden, 387 U.S. 294, 312-25 (1967) (Douglas, J., dissenting).

[54] *See* Camara v. Municipal Court, 387 U.S. 523, 535-39 (1967).

[55] In its broadest context, the term "liberty" encompasses an individual's right of autonomy—the right to live one's life without arbitrary interference by the state. *See* Louis Henkin, *Privacy and Autonomy*, 74 COLUM. L. REV. 1410, 1415 (1974).

[56] *See* Tracey Maclin, *The Decline of the Right of Locomotion: The Fourth Amendment on the Streets*, 75 CORNELL L. REV. 1258, 1297-1307 (1990).

[57] Olmstead v. United States, 277 U.S. 438, 478 (1928).

[58] *Id.* at 488 ("Under the principles established and applied by this court, the Fourth Amendment safeguards against all evils that are like and equivalent to those embraced within the ordinary meaning of its words.").

[59] See California v. Hodari D., 499 U.S. 621, 634 (1991) (Stevens, J., dissenting) ("Significantly, in the *Katz* opinion, the Court repeatedly used the word 'seizure' to describe the process of recording sounds that could not possibly have been the subject of a common-law seizure."). Furthermore, the *Terry* Court "concluded that the word

extended the scope of the Amendment to encompass temporary detentions falling short of full custodial arrests. Together, *Katz* and *Terry* emphasized a result—an intrusion upon privacy or liberty—in place of the previous focus on whether a particular means, such as trespass or arrest, had been utilized to bring about that result.

Under the specific facts of *Terry*, the relevant liberty interest was the citizen's freedom from a pat down. While concentrating on that limited issue, the *Terry* Court rose above the precise facts of the case by reaffirming its "traditional responsibility to guard against police conduct which is overbearing or harassing, or which trenches upon personal security."[60] *Terry*, like *Katz*, freed the Amendment from restrictive common law factual predicates and evoked the expansive concept of the right to be free from arbitrary governmental interference with our lives. In contrast, the *Hodari D.* Court insisted that common law concepts of arrest restrict the definition of seizures of a person.[61] This holding discards *Terry*'s broad pledge to scrutinize the diverse ways in which the government may repress a citizen's liberty in favor of giving *Terry* its narrowest reading. According to *Hodari D.*, the precise facts that gave rise to the *Terry* decision—the government's corporeal restraint of the suspect's physical movements—have become an absolute requirement for defining Fourth Amendment seizures of a person.[62] If *Terry* represents the most expansive view of Fourth Amendment protections of liberty, *Hodari D.* constitutes the most restrictive view. Any unified theory of seizures must attempt to resolve this conflict.

III. A PROPOSAL FOR UNIFICATION

One way to unify the various tests for seizures of a person into a single coherent theory is by emulating *Katz*'s unitary approach to searches of property. While the *Katz* approach may not guarantee a correct result, it does pose the proper question by forcing the Court to look beyond common law conventions in order to resolve the modern-day conflict between personal autonomy

---

'seizure' in the Fourth Amendment encompasses official restraints on individual freedom that fall short of a common-law arrest." *Id.* at 635.

[60] Terry v. Ohio, 392 U.S. 1, 15 (1968).

[61] *Hodari*, 499 U.S. at 629.

[62] *See id.* at 637.

and collective security.[63] Starting with *Katz*'s recognition of privacy as the fundamental right to be protected by prohibiting unreasonable searches, we must next ask what is the fundamental right to be protected by prohibiting unreasonable seizures of people. The obvious answer would seem to be that personal liberty is the fundamental right that the Amendment seeks to protect. Thus, the Court could quickly reconcile searches of property with seizures of persons by recognizing that a seizure occurs whenever the government infringes upon a reasonable expectation of liberty. This quick fix does provide a laudable maxim to place on coins of the realm—"We trust in God and in our reasonable expectations of privacy and liberty!" But the "fix" would likely generate much of the same criticism leveled at *Katz* for discarding concrete factors like physical trespass and tangible objects, while replacing them with high sounding but difficult to apply abstractions. The challenge the judiciary has faced in applying *Katz* is apparent from the variety of definitions of privacy suggested to courts—definitions that range from the sublime to the whimsical.[64]

Although defining liberty is likely to prove as difficult as defining privacy, focusing on the fundamental but abstract value of personal liberty does not dictate ignoring all the specific practical considerations the Court grappled with in *Mendenhall*, *Brower*, and *Hodari D.*. We can learn from the Court's consideration of the specific tests addressed in these cases, so long as these tests are not regarded as the end result, but as the means used to arrive at a general and consistent theory of Fourth Amendment seizures. Thus, it is legitimate to consider, as *Hodari D.* does, the history of common law arrests, but rather as a factor in defining seizures, not the exclusive answer. A meaningful unified theory of seizures must blend practical considerations, including our common law heritage, with broader concerns raised by modern day issues like the war on drugs and the war on terrorism.

---

[63] See, for example, Justice Harlan's approach to the constitutionality of unregulated electronic monitoring. Justice Harlan maintained that such practices:

> [U]ndermine that confidence and sense of security in dealing with one another that is characteristic of individual relationships between citizens in a free society. . . . Were third-party bugging a prevalent practice, it might well smother that spontaneity – reflected in frivolous, impetuous, sacrilegious and defiant discourse – that liberates daily life. . . . All these values are sacrificed by a rule of law that permits official monitoring of private discourse limited only by the need to locate a willing assistant.

United States v. White, 401 U.S. 745, 787-89 (1971) (Harlan, J., dissenting).

[64] For example, privacy encompasses the right to "mental and spiritual development . . . happiness, peace of mind, the proper unfolding of personality . . . ." John J. Flynn, *Tribute: Daniel J. Dykstra—The Utah Years 1949-1965*, 2000 UTAH L. REV. 831, 839 (2000) (quoting Daniel J. Dykstra, *The Right Most Valued by Civilized Man*, 6 Utah L. Rev. 305 (1959))right "to deviate temporarily from social etiquette when alone or among intimates, as by putting feet on desks, cursing, letting one's face go slack, scratching wherever one itches." Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's*, 66 COLUM. L. REV. 1003, 1025 (1966). The most commonly accepted definition is the right of individuals "to determine for themselves when, how, and to what extent information about them is communicated to others." U.S. Dep't. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 n.16 (1989).

In formulating a theory that is both theoretically sound and practical, *Katz* once again serves as a useful model in its rejection of an unrealistically expansive view of the Fourth Amendment that would regulate all government interference with privacy.[65] The Court must similarly reject an extreme view purporting to regulate all government limitations on liberty, or else we would live in a world where the government could not establish one-way streets, erect traffic signals, or post no-trespassing signs on the White House lawn. If we are to have order, not anarchy, in our society, we must accept some government restraint of our liberty, just as we accept some interference with our privacy. But putting aside any unrealistically expansive view of liberty does not force us to accept *Hodari D.*'s unduly restrictive view of liberty—that the Fourth Amendment is totally inapplicable until the government achieves total control of a citizen's movement.[66]

The problem with *Hodari D.*'s absolutist view of attempted seizures is that it places all unsuccessful government pursuit of citizens beyond the coverage of the Fourth Amendment. As the dissent queried in *Hodari D.*, are police constitutionally free to shoot at a citizen so long as they miss?[67] Bringing police pursuit and other forms of attempted seizures within the Amendment's coverage means rejecting the rigidity of *Hodari D.* and returning to the flexibility that *Terry* first injected into the Fourth

---

[65] *See* Katz v. United States, 389 U.S. 347, 350-51 (1967) (stating that "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy'").

[66] *See Hodari*, 499 U.S. at 629.

[67] *Id.* at 629-48 (Stevens, J., dissenting).

Amendment. Police pursuit impacts or limits liberty, even if it does not completely eliminate it. While some limitations on freedom of movement, like one-way streets, must be regarded as constitutionally reasonable, there is a fundamental difference between the minor inconvenience imposed by a one-way street sign and the limitations on liberty imposed by government pursuit of a citizen. The difference lies in the government's purpose because only pursuit manifests the government's intent to completely control all movement by a citizen. Thus, *Brower*'s concern for police intent can play a helpful role in defining seizures, although it should not retain its prominence as the sine qua non of that definition. The proper, but limited, role for *Brower*'s focus on government intent is to modify *Hodari D.*'s approach to attempted seizures.

A proper blending of *Brower* and *Hodari D.* would mean that when the government intends total control of the citizen and takes action that significantly impacts the citizen's liberty, the Fourth Amendment should be made applicable to this *partial seizure*. Terminology is important here because, by labeling pursuit as a mere *attempted seizure*, the Court fixates on the government's failure to achieve complete control, while ignoring its success in achieving partial control. A partial, but significant, limitation on a citizen's liberty should have constitutional consequences when it is accompanied by government intent to remove all of the citizen's freedom of movement. This blended approach rejects *Hodari D.*'s insistence that there are no constitutional consequences of an attempted, but failed, effort to seize a citizen. By rejecting *Hodari D.*, the Court could return to *Terry*'s recognition of the constitutional significance of degrees of control falling short of custodial arrests. In *Terry*'s words, a seizure occurs "when the officer, by means of physical force or show of authority, has in *some way* restrained the liberty of a citizen."[68] The uncompromising approach of *Hodari D.* accepts what the government argued, and what the Court rejected, in *Terry*—short of full arrest, infringements on privacy and liberty are mere petty indignities not covered by the Amendment.[69]

---

[68] Terry v. Ohio, 392 U.S. 1, 19 n.16 (1968) (emphasis added).

[69] *Id.* at 10-11.

This proposed blending of *Brower* and *Hodari D.* would bring attempted seizures within Fourth Amendment coverage whenever there is an intent to totally control the citizen and at least partial success in achieving that control. The next task is to address how a unified theory could alter the Court's approach to *accidental seizures*. In *Brower*, Justice Scalia posed and answered a hypothetical to test any Fourth Amendment theory purporting to cover accidental seizures: "Thus, if a parked and unoccupied police car slips its brake and pins a passerby against a wall, it is likely that a tort has occurred, but not a violation of the Fourth Amendment." [70] Justice Scalia explained that, "In sum, the Fourth Amendment addresses 'misuse of power,' not the accidental effects of otherwise lawful government conduct." [71]

The question Justice Scalia did not address is why he cares so deeply about underlying intent, even when his *Hodari D.* test for a completed seizure has been satisfied. It seems paradoxical to hold in *Hodari D.* that the Amendment is oblivious to the government's intent to seize so long as the government is unsuccessful, yet when the government is successful in eliminating the citizen's liberty, somehow the previously irrelevant intent of the government now suddenly becomes crucial. The Justice's explanation that the Fourth Amendment seeks to control deliberate government conduct, not accidents, is an incomplete answer. This explanation merely invokes one fundamental purpose of the Amendment—the need to control potentially arbitrary government conduct. The legitimacy of this purpose was best illustrated in *Delaware v. Prouse*, where the intrusion upon privacy and liberty was regarded as de minimis, but the absence of procedural controls on potentially arbitrary government power made the random stopping of an automobile constitutionally unreasonable. [72]

In isolation, *Prouse* is an important articulation of the Fourth Amendment's fundamental concern with procedural correctness. But *Prouse* cannot be viewed in isolation. It must be complimented by the considerations raised in *Winston v. Lee*, where all proper procedures were followed, but the intrusion upon privacy was far from de minimis. [73] In *Winston*, the government's efforts to remove a bullet from the defendant's body took place only after the defendant was accorded "a full measure of *procedural* protections."[74] In fact, the government bent over backwards to give the defendant the benefit of procedures exceeding those required by the Amendment—the defendant was present and represented by counsel at several evidentiary court hearings; those hearings were ultimately reviewed by the Virginia Supreme Court and by federal courts[75]—and full probable cause was established as to the likely presence of the sought-after bullet.[76] Nonetheless, the substantive requirements of the Reasonableness Clause, requirements unrelated to the procedural standards of the warrant clause, rendered the planned operation unconstitutional.[77] To the *Winston* court, "A compelled surgical intrusion into an individual's body for evidence . . . implicates expectations of privacy and security of such *magnitude* that the intrusion may be 'unreasonable' even if likely to produce evidence of a crime."[78]

---

[70] Brower v. County of Inyo, 489 U.S. 593, 596 (1989).

[71] *Id.* (citation omitted).

[72] 440 U.S. 648, 663 (1979).

By ignoring *Winston*, Justice Scalia's concern for what the government intends and his lack of concern for any harm the government accidentally causes to citizens reduces the Fourth Amendment to procedural protections. Such an approach affords no weight to the magnitude of privacy or liberty interests actually invaded by the government. When addressing accidental seizures, the Justice and his brethren would do well to consider *Winston* and *Ex rel. Francis*,[79] a case involving what may be the most famous accident in criminal procedure.

---

[73] Winston v. Lee, 470 U.S. 753, 762-63 (1985).

[74] *Id.* at 763 (emphasis added).

[75] *Id.* at 763 n.6 (noting that "the State has afforded respondent the benefit of a full adversary presentation and appellate review").

[76] *Id.* at 763.

[77] *See generally* Ronald J. Bacigal, *Dodging a Bullet, but Opening Old Wounds in Fourth Amendment Jurisprudence*, 16 SETON HALL L. REV. 597 (1986).

[78] *Winston*, 470 U.S. at 759 (emphasis added). The Court went on to say:

> In this case, however, the Court of Appeals noted that the Commonwealth proposes to take control of respondent's body, to 'drug this citizen—not yet convicted of a criminal offense—with narcotics and barbiturates into a state of unconsciousness,' . . . and then to search beneath his skin for evidence of a crime. This kind of surgery involves a virtually total divestment of respondent's ordinary control over surgical probing beneath his skin.

Id. at 765 (quoting Lee v. Winston, 717 F.2d 888, 901 (1983) (citation omitted)).

In *Francis*, the defendant was placed in the electric chair and the executioner threw the switch, but because of some mechanical difficulty, death did not result.[80] The defendant was removed from the electric chair, returned to prison, and rescheduled for execution.[81] The defendant then claimed that a second attempt at execution would violate the Fifth Amendment's protection against double jeopardy and the Eight Amendment's prohibition of cruel and unusual punishment.[82] When the case reached the U.S. Supreme Court, four Justices lamented the unfortunate circumstances of the case, but anticipating Justice Scalia's approach, they held that "[a]ccidents happen for which no man is to blame."[83] Four other Justices insisted that the State of Louisiana was engaging in cruel and unusual punishment because "[t]he intent of the executioner cannot lessen the torture or excuse the result."[84] The Justices neglected to cite, but gave full effect to, a famous maxim: "Though boys throw stones at frogs in jest, the frogs die in earnest."

Justice Frankfurter broke the four-to-four tie by approving a second attempt at execution—what the four dissenters referred to as "death by installments."[85] At least to the frogs, Justice Frankfurter clearly got it wrong. The dissenters' focus on results, not intent, serves as a model that should be applied to accidental seizures. If a citizen is under the complete control of government agents, it is difficult to regard this as a non-seizure merely because the government did not mean it. Applying *Brower* to hypothetical facts almost as gruesome as those in *Francis* means that if a pursuing police car accidentally hit and killed a fleeing citizen, there would be no seizure because the police only intended to stop the citizen by means of their siren and flashing lights. The proposed unified theory of seizures would avoid such a result by holding that there is no role for *Brower* when the government completely—intentionally or otherwise—eliminates the citizen's freedom of movement.

---

[79] Louisiana *ex rel.* Francis v. Resweber, 329 U.S. 459 (1947).

[80] *Id.* at 460.

[81] *Id.* at 461.

[82] *Id.* at 461-62.

[83] *Id.* at 462.

[84] *Id.* at 477 (Burton, J., dissenting).

[85] *Id.* at 474.

IV. A ROLE FOR *MENDENHALL*?

So far, *Hodari D.* and *Brower* have been modified and blended into a unified theory of seizures. The remaining task is to address whether *Mendenhall* has any part to play in this unified theory.[86] At present, it is unclear if the *Mendenhall* test is required when *Brower* and *Hodari D.* are satisfied. Consider this scenario: the police intend to seize a citizen, make a show of authority, and the citizen submits, thus satisfying both *Brower* and *Hodari D.* Has a Fourth Amendment seizure occurred, or is there an additional requirement that the show of authority not only enticed a particular individual to surrender liberty, but also would have convinced a reasonably prudent person that he was not free to leave?

The proposed unified theory would resolve this uncertainty by holding that the reality of actual submission should trump perceptions, thus there would be no need for the *Mendenhall* test. When there is a show of authority[87] intended to control a citizen, and it successfully achieves that control by the citizen's submission, why should the courts focus on hypothetical persons, while ignoring the very people who surrendered their liberty? The Fourth Amendment should address situations where the government actually succeeded in its planned seizure, even if it would not have succeeded against a hypothetically more reasonable and defiant citizen. If *Mendenhall* remains a vital part of the Court's approach to seizures, then no seizure occurs if a reasonable citizen would be brave enough to walk away from the police show of authority and say, "You don't scare me!" By adopting this image of a reasonably brave citizen as the sole standard to be applied, the Court turns a deaf ear to less assertive citizens who actually, although perhaps not reasonably or wisely, relinquish their liberty. This cavalier approach encourages the government to take advantage of the weaker members of our society by limiting constitutional protection to those already capable of protecting themselves by standing up to a show of government authority.

---

[86] *See* United States v. Mendenhall, 446 U.S. 544, 554 (1980).

[87] *Mendenhall's* reasonable perceptions test is only relevant to the submission prong of *Hodari D.*, not the actual touching aspect of *Hodari D.* Perceptions, reasonable or otherwise, are irrelevant when police physically control the defendant. *See* EDWIN FISHER, LAWS OF ARREST 52-53 (Robert L. Donigan ed., 1967) ("[A]n unconscious person may be placed under arrest when his body is actually seized and restrained, even though his *understanding* of his plight is delayed until he recovers consciousness.").

In the past few years, a great deal of attention has been given to the problems of bullying. Major initiatives have sought to eliminate or at least reduce bullying in our schools, where young children may not be strong enough to stand up for themselves. What counter-message is being sent when courts permit police to bully our weaker citizens into submission? It is precisely the weaker among us who are most in need of protection from the powerful, and neither private nor public bullies should be tolerated.

Consider the difference when applying the hypothetical reasonably prudent person perspective and the actual person perspective to a famous duo with very different amounts of power and perhaps fortitude—Monica Lewinski and Bill Clinton. Suppose the special prosecutors made a show of authority by stating to each of them, "Come with us now and submit to interrogation or we'll get the grand jury to indict you." I am not sure how a hypothetical reasonably prudent person might respond to this show of authority, but I can better appreciate how the actual people might respond. A Rhodes scholar, trained in the law and occupying the most powerful office in the world, is not likely to cave in to such threats. I could understand a quite different reaction from a frightened twenty-three-year-old intern.

Hodari D. requires that the police achieve successful control of the citizen in order to trigger Fourth Amendment protections.[88] If control is the sine qua non of seizures, why should actual control be disregarded in favor of *Mendenhall*'s musing about hypothetical reasonable persons? Under the proposed unified theory of seizures, there is no need for the *Mendenhall* test. When the government intentionally and successfully intimidates citizens into surrendering their liberty, the Amendment should not distinguish between citizens on grounds of their bravery or timidity, nor their reasonable or unreasonable fear of government authority.

---

[88] California v. Hodari D., 499 U.S. 621, 625-26 (1991).

CONCLUSION: THE PROPOSED UNIFIED THEORY

With apologies to Albert Einstein and Stephen Hawking, here is a concise finalized theory governing seizures of the person.

When the government totally controls a citizen's freedom of movement, in which *Hodari D.* is satisfied, there is no need for the *Brower* or *Mendenhall* tests. The reality of government control of a citizen outweighs both the perceptions of reasonably prudent people and the intent of government agents. Accidental seizures should be covered by the Amendment.

If the government achieves only partial control, such as control that causes the citizen to lose some liberty or freedom of movement by pursuing him, then there is a role for both *Brower* and *Hodari D.* When the government seeks to establish total control of the citizen, in which *Brower* is satisfied, then *Hodari D.* should be modified to recognize that even a partial loss of liberty has constitutional significance. Thus, attempted seizures would be brought within the coverage of the Amendment.

My proposed unified theory discards *Mendenhall*, but utilizes *Brower* and *Hodari D.*, not as separate definitions of a seizure, but as a means of analysis to identify the singular approach first put forth in *Terry*. The proposed unified theory thus comes full circle to end where *Terry* began—the Fourth Amendment applies when the government "has in some way restrained the liberty of a citizen."[89]

---

[89] Terry v. Ohio, 392 U.S. 1, 20 n.16 (1968).

CHALLENGES TO *TERRY* FOR THE TWENTY-FIRST CENTURY

Richard E. Myers II[*]

INTRODUCTION....937
I. *TERRY* AND REASONABLE AND ARTICULABLE SUSPICION....940
II. NEW THINGS TO ARTICULATE WITHIN THE EXISTING PARADIGM....946
  A. A Lawyer's Standard....946
  B. The Underlying Scientific Claim: Precognitive Facial Expression....948
  C. A Common Fact Pattern....951
  D. The Nose of the Camel—TSA Adopts SPOT....954
III. SOME HIDDEN FLAWS OF THE *TERRY* PARADIGM....956
  A. Naturalistic Decision Making....957
  B. Constructed Memory and Verbal Overshadowing: Going From That's How It Must Have Happened to That's How It Did Happen....959
IV. WHAT POLICY IMPLICATIONS SHOULD WE DRAW FROM THESE INSIGHTS?....963
  A. Enforcement of the Standard....965
VI. CAMERAS AS A SOLUTION....967
CONCLUSION....970

INTRODUCTION

"Reasonable and articulable suspicion" is generally understood as the Fourth Amendment standard the Supreme Court chose in *Terry v. Ohio*[1] as the basis for brief investigative stops by police officers. Articulable suspicion is a lawyer's standard. Judges—and lawyers generally—are partial to words, which are their stock-in-trade. But much of what matters to people in the world is incredibly difficult to reduce to language. Moreover, many people, including some otherwise talented police officers, may lack the linguistic capacity to successfully recount their experiences in language that lawyers and judges can use in court. This Article considers the portion of the "totality of the circumstances" that lies beyond the articulable, exploring the limitations of witness testimony regarding fast-moving events, and the ways in which technology will alter the margins of practice on the street and in the courtroom.

---

[*] George R. Ward Associate Professor of Law, UNC School of Law. My research assistants, Lorelle Babwah, Andrew Kasper, and Matthew Nigriny provided invaluable assistance. Christopher Slobogin, Ronald Wright, Donald Dripps, Dan Markel, and my UNC faculty colleagues improved the article with thoughtful advice.

[1] 392 U.S. 1, 30 (1968).

As this Article is being written, the background understandings of human cognition and its effect on police practice are shifting. Emerging science on cognitive processes is introducing new challenges into the courtroom. On the one hand, some social scientists are explaining human behavior in ways that make it possible for law enforcement officers to translate their heretofore inarticulable experiences into words. On the other, the findings of other scientists who study the nature of expertise suggest that the traditional *Terry* inquiry, with its focus on conscious thought, may be missing much of the picture. Expert police officers process much of the critical information on which they rely at a subconscious—and therefore inarticulable—level. The better they get at their job, the less likely they are to make conscious note of classes of information, especially in the potentially life-threatening situations that may lead to frisks for weapons. Additionally, the process of preparing for the *Terry* test may be driving some information out of police officers' memories, at the same time it seeks to capture other information. Police officers, as much as, and perhaps more than other eyewitnesses, are susceptible to verbal displacement.

And officer memory may not be the best evidence available. In the twenty-first century, digital recorders are proliferating—they can be found in police cars, on officers' lapels, on witness cell phones, in retail security systems, the list expands daily. These technological advances are making it possible for many officers, and many suspects, to bring video or audio recordings of their experiences to court. Fourth Amendment doctrine must explicitly make room for these technological advances. If, as this Article argues, "reasonable and articulable" suspicion is really a subset of "reasonable suspicion based on credible evidence," then digital video and audio recordings should serve as a new, affordable, and widely available adjunct to officer testimony that fits nicely into this broader doctrinal framework.

This Article proceeds in four parts. Part I examines briefly the legal regime established by the Supreme Court and commonly referred to by the name of the seminal case, *Terry v. Ohio*, and suggests that the totality-of-the-circumstances approach adopted by the Court is broader than the traditional "reasonable and articulable suspicion" formulation.[2] Part II examines some of the developments in cognitive science that have implications for the application of the *Terry* standard. It examines new law enforcement applications of the emerging science of precognitive facial expression, which makes the previously inarticulable articulable. This new application is changing the landscape underneath *Terry*. It then looks at the naturalistic decision-making literature, a branch of psychology of expertise, and suggests that *Terry* may be asking a question that is poorly suited to the environment in which officers operate, and to the nature of their expertise. It finally considers some recent research on witness memory, and suggests that the process of preparing to meet the *Terry* standard may be introducing to the courtroom inaccuracies that are real, albeit difficult to quantify. Part III briefly considers some of the policy implications of the interaction between cognitive science and police conduct under the *Terry* regime. It suggests that the protection offered under the *Terry* standard may be slowly eroding, even as its presence may be creating a false sense of confidence that "the courts" are the answer to the age-old query, "Who watches the watchers?"[3] Part IV considers the viability of digital video as an adjunct to or substitute for officer testimony. We may have a new answer to who watches: the digital video camera.

---

[2] *Id.*

[3] Commonly attributed to the plays of Juvenal, the question in Latin is *Quis custodies ipsos custodiet.*

I. *TERRY* AND REASONABLE AND ARTICULABLE SUSPICION

The language "reasonable and articulable suspicion" is immediately familiar to any student of criminal procedure.[4] It is the Fourth Amendment standard[5] articulated by the Supreme Court in the *Terry* line of cases as the minimum basis required for brief investigative stops by police officers. These brief, investigative "*Terry* stops"[6] are police-citizen encounters short of a full arrest, but where appropriate they may include a "frisk" for weapons.[7] As this Section will show, the courts have given increasing deference to the police regarding the bases for such stops, but they have retained their prerogative to review police behavior, even if the standard is more deferential than probable cause. "The stop and frisk rule permits the police to engage in what most people regard as reasonable and essential law enforcement activity but requires them to pay attention to all of the circumstances they confront and to articulate a reason for their actions that may be judicially reviewed."[8]

Courts applying the *Terry* standard in its current state of evolution may consider a broad range of suspect conduct, such as nervousness, evasive behavior, flight, and responses to questions.[9]

> In reviewing the propriety of an officer's conduct, courts do not have available empirical studies dealing with inferences from suspicious behavior, and this Court cannot reasonably demand scientific certainty where none exists.

---

[4] For an excellent discussion of the rise of the *Terry* standard, see Stephen A. Saltzburg, Terry v. Ohio: *A Practically Perfect Doctrine*, 72 ST. JOHN'S L. REV. 911 (1998).

[5] The Fourth Amendment states, in full:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S CONST. amend. IV.

[6] *See generally* WAYNE R. LAFAVE, 1 SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 9.1 (4th ed. 2009).

[7] A frisk is a limited pat-down of the outer clothing of a suspect to check for weapons. *Id.* at 5. If an object that might be a weapon is felt under a suspect's clothing, it can be removed for visual examination. *Id.*

[8] Salzburg, *supra* note 4, at 962.

[9] LAFAVE, *supra* note 6.

> Thus, the reasonable suspicion determination must be based on commonsense judgments and inferences about human behavior.[10]

In *Terry* itself, Martin McFadden, a police officer with thirty-nine years of experience as a Cleveland police officer, observed three men who were, in his estimate, "casing a job, a stick-up."[11] McFadden described the elaborate sequence of events in which the men walked back and forth in front of a store for ten to twelve minutes, and stopped on the corner to talk with a third man, before returning to once again stare into the window.[12] The police officer stopped the men, and asked them some questions.[13] Worried for his safety, he quickly frisked the men for weapons by patting down their outer clothing, and felt concealed firearms on two of them.[14] The men were arrested and convicted on weapons charges.[15]

Terry's appeal was based on the absence of probable cause to arrest him.[16] The Court, in an opinion written by Justice Warren, agreed, but held that the absence of probable cause was not the end of the inquiry.[17] The government argued that such encounters—because they fell short of full arrest—were outside the purview of the Fourth Amendment.[18] Justice Warren wrote that the Fourth Amendment did apply, but that there was an

> entire rubric of police conduct—necessarily swift action predicated upon the on-the-spot observations of the officer on the beat—which historically has not been, and as a practical matter could not be, subjected to the warrant procedure.[19] Instead, the conduct . . . must be tested by the

---

[10] Illinois v. Wardlow, 528 U.S. 119, 119 (2000).

[11] *Terry v. Ohio*, 392 U.S. 1, 6 (1968) (quoting McFadden's testimony).

[12] *Id.*

[13] *Id.* at 6-7.

[14] *Id.* at 7.

[15] *Id.* at 8.

[16] *Id.* at 25.

[17] *Id.* at 20.

[18] *Id.* at 10.

[19] *Id.* at 20.

> Fourth Amendment's general proscription against unreasonable searches and seizures.[20]

The Court further held that the standard was objective, not based on the officer's subjective good faith.[21] Judged after the fact, the circumstances must be those that would have led a reasonable person to believe that the stop and frisk were warranted.[22] Given the suspicious behavior that Officer McFadden observed, he was justified in making a brief investigative stop.[23] Moreover, the limited search for weapons that he conducted was reasonable under the circumstances.[24]

Cases since *Terry* have referred to the standard as requiring reasonable and articulable suspicion.[25] The officer must be acting on more than an "inchoate and unparticularized suspicion or 'hunch'"[26] of criminal activity, but may bring experience and training to bear to allow seemingly innocuous information to be considered as part of the totality of the circumstances. *Terry* was originally framed as a narrow exception to the Fourth Amendment requirement that officers have probable cause before searching or seizing a person or property.[27] In *Terry*, the Supreme Court empowered police officers to stop and frisk a suspect if the officer had a reasonable and articulable suspicion that "criminal activity [was] afoot" and the suspect was armed and dangerous.[28] This narrow exception, based on a standard less rigorous than probable cause, was substantially expanded in subsequent decisions, leading some commentators to express concern that the exception was beginning to swallow the rule.[29]

---

[20] *Id.*

[21] *Id.* at 21.

[22] *Id.* at 21-22.

[23] *Id.* at 23.

[24] *Id.* at 28-29.

[25] Illinois v. Wardlow, 528 U.S. 119, 123 (2000) ("In *Terry*, we held that an officer may, consistent with the Fourth Amendment, conduct a brief, investigatory stop when the officer has a reasonable, articulable suspicion that criminal activity is afoot."). Justice Harlan's language in his *Terry* concurrence most closely matches the current formulation: "Where such a stop is reasonable, however, the right to frisk must be immediate and automatic if the reason for the stop is, as here, an articulable suspicion of a crime of violence." *Terry*, 392 U.S. at 33 (Harlan, J., concurring). A Westlaw search for the phrase "articulable suspicion" in the allfeds database on August 16, 2010 yielded more than 3,800 results. A similar search in allcases hits the 10,000 result limit.

[26] *Terry*, 392 U.S. at 27.

[27] LAFAVE, *supra* note 6, § 9.1(c).

[28] *Terry*, 392 U.S. at 30 (alteration to original).

Since *Terry* was decided, the law has evolved in two key ways. First, the lower courts have expanded the original scenario, involving violent crimes or suspects thought to be armed and dangerous, to include crimes that are not inherently violent, such as burglaries and drug offenses, and to allow searches of suspects in certain cases where there is no direct evidence that the suspect is armed or dangerous.[30] Second, some observers have argued that trial courts have shown a willingness to "unquestioningly accept the testimony of police witnesses," significantly reducing the amount of evidence that will meet the standard.[31]

In a 1994 article, Professor David Harris noted that much of the expansion of *Terry* up to that point had occurred at the trial and intermediate appellate court levels, with the Supreme Court continuing to characterize *Terry* as a narrow exception to the probable cause requirement.[32] However, the Court's recent Fourth Amendment decisions appear to embrace—and arguably even expand—the broader conception of *Terry* previously adopted by the lower courts. In two of its most recent *Terry* decisions, *United States v. Arvizu*[33] and *Illinois v. Wardlow*,[34] the Supreme Court overturned lower court decisions to suppress evidence based on a restrictive view of the scope of *Terry*.[35]

---

[29] David A. Harris, *Frisking Every Suspect: The Withering of* Terry, 28 U.C. DAVIS L. REV. 1, 5 (1994); Gregory H. Williams, *The Supreme Court and Broken Promises: The Gradual But Continual Erosion of* Terry v. Ohio, 34 HOW. L.J. 567, 576-83 (1991); *see also* Michael J. Roth, Note, Berkemer *Revisited: Uncovering the Middle Ground Between* Miranda *and the New* Terry, 77 FORDHAM L. REV. 2779, 2800-03 (2009); Jamie L. Stulin, Comment, *Does* Hiibel *Redefine* Terry? *The Latest Expansion of the* Terry *Doctrine and the Silent Impact of Terrorism on the Supreme Court's Decision to Compel Identification*, 54 AM. U. L. REV. 1449, 1456-58 (2005).

[30] Harris, *supra* note 29, at 23-32.

[31] *Id.* at 33.

[32] *Id.* at 5-6.

[33] 534 U.S. 266, 268 (2002).

[34] 528 U.S. 119, 121 (2000).

[35] *Arvizu*, 534 U.S. at 277 (holding that court below incorrectly suppressed evidence from vehicle search, where border patrol officer stopped vehicle after observing defendant driving on road frequented by drug smugglers and seeing children in back seat waving oddly); *Wardlow*, 528 U.S. at 125 (holding that Illinois Supreme Court incorrectly suppressed evidence obtained during stop and frisk of defendant who ran away from police vehicle that was entering high crime area, despite police officer's inability to remember whether police car was marked or unmarked). In a third case,

While courts have substantially liberalized their inquiry under *Terry*, it remains an important cornerstone of Fourth Amendment law. Other scholars have written extensively on *Terry*.[36] It has been variously described as a "practically perfect doctrine," and as a dismal failure.[37] It has been described as revolutionary, and as evolutionary.[38] Others have suggested that the balance in *Terry* itself was correct, but that subsequent decisions have tipped the balance in favor of the police,[39] and yet others suggest that *Terry*'s strength is that it is flexible enough to move back and forth with the times.[40] Other critics have noted

---

Hiibel v. Sixth Judicial District Court, 542 U.S. 177, 191 (2004), the Court held that a state may require a suspect to disclose his name during a *Terry* stop without violating the Fourth Amendment. While the majority maintained that *Hiibel* was not inconsistent with previous *Terry* decisions, *id.* at 188, commentators have argued that *Hiibel* diverges from earlier opinions stating that suspects cannot be required to answer questions during *Terry* stops. *See* Stulin, *supra* note 29, at 1456-63. One notable exception to this trend towards an expansive interpretation of *Terry* is *Florida v. J.L.*, 529 U.S. 266 (2000), where the Court held that an "anonymous tip that a person is carrying a gun, is, without more, [in]sufficient to justify a police officer's stop and frisk of that person." *Id.* at 268.

[36] *See, e.g.*, Wayne R. LaFave, *Two Hundred Years of Individual Liberties: Essays on the Bill of Rights: Pinguitudinous Police, Pachydermatous Prey: Whence Fourth Amendment "Seizures"?*, 1991 U. ILL. L. REV. 729 (1991); Christopher Slobogin, *Let's Not Bury* Terry*: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053 (1998); Gregory H. Williams, *The Supreme Court and Broken Promises: The Gradual But Continual Erosion of* Terry v. Ohio, 34 HOW. L.J. 567, 576 (1991) (arguing that the Court struck the right balance in *Terry* but later decisions undermined that balance).

[37] *See* Tracey Maclin, *When the Cure for the Fourth Amendment is Worse Than the Disease*, 68 S. CAL. L. REV. 1, 35 (1994) (arguing that *Terry*'s rationale has been distorted to justify ever-more intrusive police conduct); Saltzburg, *supra* note 4, at 912 (arguing that *Terry* strikes a "practically perfect" balance). *See generally* Adina, Schwartz, *Just Take Away Their Guns: The Hidden Racism of* Terry v. Ohio, 23 FORDHAM URB. L.J. 317, 331 (1996) (arguing that *Terry* weakened the rights of defendants of all races when it broadened the basis for admissibility of evidence); Scott E. Sundby, *An Ode to Probable Cause: A Brief Response to Professors Amar and Slobogin*, 72 ST. JOHN'S L. REV. 1133, 1136-37 (1998) (discussing tension between individual liberties and police power).

[38] Slobogin, *supra* note 36, at 1095 ("*Terry* didn't alter law enforcement practices; it just provided, in the hands of the post-Warren Court, a rationale for the status quo.").

[39] Williams, *supra* note 36, at 576 (arguing that the Court struck the right balance in *Terry* but later decisions undermined that balance).

[40] *See* Craig S. Lerner, *Judging Police Hunches*, 4 J.L. ECON. & POL'Y 25, 39-40 (2007); Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of* Camara *and* Terry, 72 MINN. L. REV. 383, 402 (1988) ("[R]easonable suspicion became a valid compromise standard that comports with the [F]ourth [A]mendment if the Court decides that, after balancing the interests, it is reasonable. The government

that different and even contradictory information has been accepted by trial courts as an acceptable basis for an investigative stop, leading to a perception of oversight, even though the courts are simply ratifying officers' judgments so long as they offer any justification for their actions.[41]

Since *Terry* was decided, the courts have emphasized that the issue is a practical one. In *United States v. Cortez*,[42] Chief Justice Burger, writing for the majority, emphasized the inherent difficulties that come with applying the standard, and also recognized that the courts would give deference to the particularized training of police officers:

> Courts have used a variety of terms to capture the elusive concept of what cause is sufficient to authorize police to stop a person. Terms like "articulable reasons" and "founded suspicion" are not self-defining; they fall short of providing clear guidance dispositive of the myriad factual situations that arise. But the essence of all that has been written is that the totality of the circumstances—the whole picture—must be taken into account. Based upon that whole picture the detaining officers must have a particularized and objective basis for suspecting the particular person stopped of criminal activity.
>
> The idea that an assessment of the whole picture must yield a particularized suspicion contains two elements, each of which must be present before a stop is permissible. First, the assessment must be based upon all of the circumstances. The analysis proceeds with various objective observations, information from police reports, if such are available, and consideration of the modes or patterns of operation of certain kinds of lawbreakers. From these data, a trained officer draws inferences and makes deductions—inferences and deductions that might well elude an untrained person.

---

no longer argues against a presumed starting point of probable cause but rather argues for reasonable suspicion as a reasonable accommodation of competing interests.").

[41] Charles L. Becton, *The Drug Courier Profile: "All Seems Infected that th' Infected Spy, As All Looks Yellow to the Jaundic'd Eye,"* 65 N.C. L. REV. 417, 444-47 (1987).

[42] 449 U.S. 411 (1981).

> The process does not deal with hard certainties, but with probabilities. Long before the law of probabilities was articulated as such, practical people formulated certain common sense conclusions about human behavior; jurors as factfinders are permitted to do the same—and so are law enforcement officers. Finally, the evidence thus collected must be seen and weighed not in terms of library analysis by scholars, but as understood by those versed in the field of law enforcement.
>
> The second element contained in the idea that an assessment of the whole picture must yield a particularized suspicion is the concept that the process just described must raise a suspicion that the particular individual being stopped is engaged in wrongdoing. Chief Justice Warren, speaking for the Court in *Terry v. Ohio*, supra, said that "[t]his demand for specificity in the information upon which police action is predicated is *the central teaching of this Court's Fourth Amendment jurisprudence*."[43]

II. NEW THINGS TO ARTICULATE WITHIN THE EXISTING PARADIGM

A. A Lawyer's Standard

Make no mistake; articulable suspicion is a lawyer's standard. Judges—and lawyers generally—have an inherent bias in favor of words.[44] Words are the lawyer's stock-in-trade. Ordinarily, experiences that cannot be reduced to words cannot be explained in a way that makes them available as evidence in court, and they are unreviewable by appellate judges, who depend on a written record. Lawyers are trained for years in the art of rearranging emotional responses to issues into legal arguments, to use the language of the law to reinterpret their prior experience so that it fits into the existing structure. One shortcoming inherent in a language-based system is that much of what matters to people in the world is incredibly difficult to reduce to language. Another is that many people lack the linguistic capacity to cast their experiences, no matter how real they have been, in language that lawyers and judges can use in court. It naturally creates biases in favor of the articulable portion of experience, and the articulate portion of the population.

---

[43] *Id.* at 417-18 (citations omitted) (quoting Terry v. Ohio, 392 U.S. 1, 21 n.18 (1968)).

[44] *See* Lerner, *supra* note 40, at 25 ("The legal system in practice rewards those officers who are able and willing to spin their behavior in a way that satisfies judges, while it penalizes those officers who are less verbally facile . . . .").

The world of *Terry* is undergoing an important change. Whether and how much that change will ultimately affect the gross number of searches that the courts allow to meet the *Terry* standard remains to be seen. Nonetheless, social scientists such as Paul Ekman in the area of facial expression of emotion[45] and Ray Bull and Aldert Vrij in the science of distinguishing truth from lies,[46] are creating a scientific framework that makes it possible for law enforcement officers to translate their previously unexplained experiences into words. Training in their methods will make it possible for the police to introduce heretofore inaccessible evidence regarding their experiences in court. If judges credit the new science, more searches will meet the reasonableness threshold.

How many cases this will affect is impossible to predict. Some courts already have been willing to accept vague language about facial expression and behavior because they understand that describing in detail how someone looks and acts can be challenging. Paul Ekman and the other social scientists who have adopted or adapted his methods for studying human expression and emotion have created a system that permits highly specific description of observed facial expression. Ekman's system has the potential to change the way people, including the police, perceive and describe people's facial expressions. The Facial Action Coding System Ekman and Wallace Friesen created has more than fifty possible components of an expression.[47] The components of an expression are created by the contraction of numerous facial muscles, some of which most people have conscious control over, and some of which most people leave to their autonomic muscles. The example Ekman uses is the difference between the "Pan-American" smile, the say-cheese smile that has appeared in photo albums everywhere, looks posed and never reaches the eyes, and a genuine smile, which activates different muscles[48] around the nose and eyes.[49] Many people can tell the difference between a true smile and a false smile. Far fewer have the training or the vocabulary to explain why one was false and the other was not.

---

[45] *See infra* at notes 47-67 and accompanying text; *see also* PAUL EKMAN, EMOTIONS REVEALED: RECOGNIZING FACES AND FEELINGS TO IMPROVE COMMUNICATION AND EMOTIONAL LIFE (2d ed. 2003) [hereinafter EMOTIONS REVEALED]; PAUL EKMAN, TELLING LIES: CLUES TO DECEIT IN THE MARKETPLACE, POLITICS AND MARRIAGE (3d ed. 2001) [hereinafter TELLING LIES]. Ekman's work, and its possible applications police investigations, has been explored recently in the television series *Lie to Me*. According to his website, he "frequently advises police departments, anti-terrorism groups, and animation studios." *See The Truth Behind the Lies: Evening Seminar*, SMITHSONIAN RESIDENT ASSOCIATES PROGRAM, http://residentassociates.org/ticketing/tickets/reserve.aspx?performanceNumber=219398 (last visited Nov. 1, 2010).

[46] *See, e.g.*, ALDERT VRIJ, DETECTING LIES AND DECEIT: THE PSYCHOLOGY OF LYING AND ITS IMPLICATIONS FOR PROFESSIONAL PRACTICE (2000); Aldert Vrij, *Criteria-Based Content Analysis: A Qualitative Review of the First 37 Studies*, 11 PSYCHOL. PUB. POL'Y & L. 3 (2005); Aldert Vrij, Katherine Edward & Ray Bull, *Stereotypical Verbal and Nonverbal Responses While Deceiving Others*, 27 PERS. & SOC. PSYCHOL. BULL. 899 (2001).

Subject those untrained people to skilled cross-examination in a courtroom, and the results will not be pretty. But give them some training, and things might change considerably. The officer who previously thought something was not right will be able to explain what it was that he saw that was not right. Instead of the processing taking place subconsciously, it can be moved to the conscious level. This has implications under *Terry* because it will allow the basis for suspicion to be articulable.

B. The Underlying Scientific Claim: Precognitive Facial Expression

The basic scientific claims underlying the science of precognitive facial expression are fairly simple and somewhat intuitive. First, basic facial expressions related to human emotion are biologically, not socially determined.[50] They are "hardwired" and are the same across cultures, barring some abnormality.[51]

---

[47] PAUL EKMAN & WALLACE V. FRIESEN, THE FACIAL ACTION CODING SYSTEM (1978).

[48] EKMAN, TELLING LIES, *supra* note 45, at 150-51.

[49] Errol Morris, *The Most Curious Thing*, NYTIMES.COM (May 19, 2008 10:56 PM), http://opinionator.blogs.nytimes.com/2008/05/19/the-most-curious-thing/; *see also* EKMAN, EMOTIONS REVEALED, *supra* note 45, at 204-12.

[50] EKMAN, EMOTIONS REVEALED, *supra* note 45, at 2-14.

[51] *Id.*

Babies smile when they are happy, not because they have learned to smile from watching their parents, but because they have instinctive physiological responses.[52] Second, people's emotions are revealed on their faces via involuntary muscular contractions, and these facial expressions occur precognitively, before the individual becomes consciously aware that they are experiencing the emotion.[53] Once the individual is aware that they are experiencing the emotion, they can regain control of their facial expressions,[54] hence the term "fleeting expression." There are some limits to this. People can artificially limit their facial expressions in advance by adopting a "poker face." While it is hard to mask genuine emotions, it is also difficult to voluntarily mimic genuine facial expressions of emotion.[55] It is hard for most people to voluntarily contract a subset of the facial muscles that are naturally involved in genuine expressions.[56] Because autonomic systems control those responses, a smile that comes from genuine emotion is in fact different in appearance from a forced smile.[57]

Perhaps less intuitive is a third claim: with training, most people can see and identify the fleeting expressions, and can detect and articulate the difference between genuine and forced expressions.[58] Some people—those with strong intuitive skills—are very good at this naturally, although they usually lack the capacity and the vocabulary to explain what it is they were doing.[59]

The science has a long intellectual history, starting with the work of Wallace Friesen,[60] and being largely systematized by Paul Ekman, a psychologist and professor who created the Facial

---

[52] This theory dates back to Darwin's observations of blind children.

[53] EKMAN, TELLING LIES, *supra* note 45, at 123-26.

[54] *Id.* at 131.

[55] *Id.* at 132-33.

[56] *Id.*

[57] *Id.* at 158-60.

[58] *See* Paul Ekman et al., *A Few Can Catch A Liar*, 10 PSYCHOL. SCI. 263, 263-65 (1999) (finding that seventy-three percent of federal intelligence and law enforcement officers, sixty-seven percent of Los Angeles County sheriffs, and sixty-two percent of federal judges could detect a lie after completing training in facial recognition methods).

[59] *Id.*

[60] Paul Ekman & Wallace V. Friesen, *Nonverbal Leakage and Clues to Deception*, 32 PSYCHIATRY 88 (1969).

Action Coding System ("FACS") for documenting the component changes in facial expression.[61] Ekman's work was popularized in science writer Malcolm Gladwell's 2005 bestseller, *Blink: The Power of Thinking Without Thinking*.[62] Ekman and some of his successors have adapted the methodology and now offer training in this science to law enforcement.[63]

In *Blink*, Malcolm Gladwell offered a tantalizing glimpse of the potential use of the science of facial expression in the courtroom when he interviewed Ekman. Ekman chose, as one example of his system, videotaped testimony from the murder trial of former University of Southern California and Buffalo Bills running back O.J. Simpson.[64] He dissected the testimony of Brian "Kato" Kaelin, an actor who rented Simpson's pool house and saw O.J. Simpson the night that his ex-wife Nicole Brown Simpson and Beverly Hills waiter Ronald Goldman were murdered.[65] Kaelin's testimony regarding Simpson's whereabouts that night and Simpson's demeanor when he encountered Kaelin shortly after the murders was important to the case. As Gladwell explains the exercise:

> Ekman slipped a tape taken from the O.J. Simpson trial into the VCR. It was of Kato Kaelin, Simpson's shaggy-haired house guest, being examined by Marcia Clark, one of the prosecutors in the case. Kaelin sits in the witness box, with his trademark vacant look. Clark asks a hostile question. Kaelin leans forward and answers softly. "Did you see that?" Ekman asked me. I saw nothing, just Kato being Kato—harmless and passive. Ekman stopped the

---

[61] EKMAN & FRIESEN, *supra* note 47.

[62] MALCOLM GLADWELL, BLINK: THE POWER OF THINKING WITHOUT THINKING 197-214 (2005).

[63] According to Ekman's website, he "frequently advises police departments, anti-terrorism groups, and animation studios." *See See The Truth Behind the Lies: Evening Seminar*, SMITHSONIAN RESIDENT ASSOCIATES PROGRAM, http://residentassociates.org/ticketing/tickets/reserve.aspx?performanceNumber=219398 (last visited Nov. 1, 2010). Customs officials report that after receiving training from Ekman their "hit rate" for finding drugs during passenger searches increased to 22.5 percent from 4.2 percent in 1998. Bob Burns, *The Truth Behind the Title: Behavior Detection Officer*, THE TSA BLOG (Feb. 29, 2008 4:12 PM), http://blog.tsa.gov/2008/02/truth-behind-title-behavior-detection.html.

[64] GLADWELL, *supra* note 62, at 211.

[65] *Id.*

> tape, rewound it, and played it back in slow motion. On the screen, Kaelin moved forward to answer the question, and in that fraction of a second his face was utterly transformed. His nose wrinkled, as he flexed his levator labii superioris, alaeque nasi. His teeth were bared, his brows lowered. "It was almost totally A.U. nine," Ekman said. "It's disgust, with anger there as well, and the clue to that is that when your eyebrows go down, typically your eyes are not as open as they are here. The raised upper eyelid is a component of anger, not disgust. It's very quick." Ekman stopped the tape and played it again, peering at the screen. "You know, he looks like a snarling dog."
>
> Ekman said that there was nothing magical about his ability to pick up an emotion that fleeting. It was simply a matter of practice. "I could show you forty examples, and you could pick it up. I have a training tape, and people love it. They start it, and they can't see any of these expressions. Thirty-five minutes later, they can see them all. What that says is that this is an accessible skill."[66]

And some police are now training to access that skill. As they do so, their reliance on it, and their testimony about it will become crucial.[67]

C. A Common Fact Pattern

Ekman's work may be giving new answers to old questions: How do good cops explain what they are doing and why they are doing it to those of us who have never been there? How is expertise in criminal behavior and the patterns of street conduct translated into language accessible by the courts? To help work through the practical implications, consider the following fact pattern: Imagine for a moment a police officer passing an individual on a crowded street late one summer night, in a bar district he regularly patrols on foot. Something about the individual he just passed strikes a chord in him somewhere, but he is not sure why. His instincts, honed by years on the street, ring an alarm bell and are screaming danger. He cannot articulate a reason. The man is dressed normally, although he is wearing a loose jacket with a bulge under his arm. His clothing is out of place for the area, which is a nightclub district, and the weather is warm. He is walking oddly, but that is not enough to have set off the officer's instincts. His face was wrong, but he can't explain what about it made him react. The man clearly appears to be looking for someone. He watches the man's back a little while longer. He imagines having to explain to his sergeant and to the courts later why he stopped the man and decides that he does not have enough information to explain why he made a stop, so he proceeds on his way. Twenty minutes later, the man shoots and kills his estranged wife. Did this officer do the right thing?

---

[66] *Id.*

[67] It also may lead to more searching than civil libertarians might be comfortable with, if it ever became a permissible sole basis for a *Terry* stop. And it has the potential to make already bad situations even worse, if we widely accept these new techniques, and give bad cops something new, and fundamentally unfalsifiable, to say in court. For the bad cops, it may make very little difference because they will lie to meet the legal standard no matter what it is. However, it may give them something to say when cameras capture many aspects of a situation but miss the suspect's face.

Now re-imagine the same scenario. At the moment the alarm bells are triggered in his head, the police officer reacts to his instinct and stops the man. He attempts to ask him questions, but the man says "If you're arresting me, arrest me, if you're not, leave me alone. I know my rights." After this very brief conversation, the officer cannot shake the feeling that the man is dangerous. The bulge that he noticed in the man's jacket is too indistinct for him to say what is in it. Although he cannot say why, he is convinced the man is dangerous. He tells the man to put his hands on top of his head, leans him against the wall, and frisks him. It turns out he is carrying a concealed weapon—a handgun, in a shoulder holster. The officer takes the man's gun, handcuffs him, and takes his wallet out of his pocket to identify him. He radios the station for information on the man, based on the ID he finds in his wallet. It turns out that the man is a convicted felon with a history of spousal battery who is under a current domestic violence restraining order. Further investigation reveals that his estranged wife was out with a date at a nightclub three blocks from the location where the man was stopped. In this jurisdiction, it is a crime to carry a concealed weapon while subject to a domestic violence restraining order, so the officer arrests the man. Did this officer do the right thing? What he did was unconstitutional under current doctrine, and the handgun would almost certainly be suppressed as the fruit of the poisonous tree.

Let us imagine the same scenario again. This time, the officer finds a flashlight in the man's coat pocket, not a concealed weapon. The officer takes the man's ID as before, writes down his name, apologizes for the inconvenience, and leaves.[68] Did this officer do the right thing?

Now let us once again imagine this scenario differently, in a world where police have extensive training in behavioral observation and a new technique—precognitive facial expression analysis, a form of applied cognitive psychology. Now, when he is asked about what he saw, the officer says that when he looked into the man's face as he was approaching him on the street, he saw a series of microexpressions or "emblematic slips." These microexpressions included anger and disgust as the man looked at women passing him on the street and mingled fear and disgust when he saw the police officer.[69] The officer explains how he was able to do so, based on his training in precognitive facial expression. The officer explains that he has been trained that there are fleeting facial expressions that appear in response to environmental stimuli, and that these expressions occur precognitively, before the individual is aware of them and consciously asserts control over his facial muscles. Because they are instinctive and precognitive, they are very effective indicators of a person's genuine emotion. In addition, the man's behavior was consistent with hunting for someone, not simply strolling down the street. He was rapidly scanning the crowd, checking faces, dismissing them, and continuing down the street. He appeared to be hyper-alert, in an area where most people were relaxed and having a good time. The officer stops and frisks the suspect based on these criteria.

---

[68] *Cf.* Bennett Capers, *Policing, Race, and Place*, 44 HARV. C.R.-C.L. L. REV. 43, 63 (2009) (noting that only one out of ten individuals stopped and frisked by the New York Police Department in 2006 were arrested or served summons); Christopher Slobogin, *Why Liberals Should Chuck the Exclusionary Rule*, 1999 U. ILL. L. REV. 363, 374 n.34 (1999) (noting that only one out of one-hundred people stopped by New Orleans police officers in the late 1960s were prosecuted).

[69] Of course, people may fear or distrust the police for many reasons. *See, e.g.*, Lenese Herbert, *Othello Error: Facial Profiling, Privacy, and the Suppression of Dissent*, 5 OHIO ST. J. CRIM. L. 79 (2007); Andrew E. Taslitz, *Police Are People Too: Cognitive Obstacles to, and Opportunities for, Police Getting the Individualized Suspicion Judgment Right*, 8 OHIO ST. J. CRIM. L. 7, 10-12.

Is this enough to change the balance? That will depend in part on the interaction between the legal standard—"reasonable and articulable suspicion" and judicial consumption of the police officer's training in the new methods. Social scientists who study human expression and emotion have created the language that will permit translation of police experience into words. We can expect a shift from cop-speak terms like "there was something 'hinky'[70] about the guy" (a statement which in this author's experience has drawn nods from experienced law enforcement officers across the country but will draw frowns from judges) to "his precognitive affect was inconsistent with his surroundings." This statement is scientifically sound, almost impossible to falsify, will include embedded value judgments about what human emotions should be showing on a person's face in a given context, and may lead to more searching than we are comfortable with if it becomes a permissible sole basis for a *Terry* stop.

D. The Nose of the Camel—TSA Adopts SPOT

The use of the science of precognitive facial expression in law enforcement is no hypothetical—it has arrived. If someone has flown into a major airport in the United States in the last three years, odds are that it has been applied to them or their traveling companions.[71] Screeners for the Transportation Safety Authority (TSA) have been applying behavioral observation techniques based on this science under the acronym SPOT (Screening Passengers by Observation Technique).[72] The techniques are based on behavior, so in theory they avoid the potential for bias that existed in profiles based on immutable characteristics.[73] Whether the immutable characteristics may be used more subtly, for example in selecting whom to observe in the first instance, is an open question.

---

[70] *See Hinky* Definition, URBANDICTIONARY.COM, http://www.urbandictionary.com/define.php?term=hinky (visited Nov. 1, 2010) (defining hinky as 1) "Something as yet undefinable is wrong, out of place; not quite right. There's something hinky about the deal[,]" or 2) "A cop's version of "I've a bad feeling about that.").

[71] *See Behavior Detection Officers (BDO): Layers of Security*, TRANSP. SEC. ADMIN., http://www.tsa.gov/what_we_do/layers/bdo/index.shtm (last visited Nov. 1, 2011) (noting that behavior detection officers (BDOs) currently are deployed at 161 airports in the United States).

[72] *See BDOs SPOT More Than Just Opportunities at TSA: News & Happenings*, TRANSP. SEC. ADMIN., (May 8, 2007), http://www.tsa.gov/press/happenings/boston_bdo_spot.shtm.

Kip Hawley, the Assistant Secretary of Homeland Security described the techniques as follows:

> We use a system of behavior observation that is based on the science that demonstrates that there are certain involuntary, subconscious actions that can betray a person's hostile intent. For instance, there are tiny—but noticeable to the trained person—movements in a person's facial muscles when they have certain emotions. It is very different from the stress we all show when we're anxious about missing the flight due to, say, a long security line. This is true across race, gender, age, ethnicity, etc. It is our way of not falling into the trap where we predict what a terrorist is going to look like. We know they use people who "look like" terrorists, but they also use people who do not, perhaps thinking that we cue only off of what the 9/11 hijackers looked like.
>
> Our Behavior Detection teams routinely—and quietly—identify problem people just through observable behavior cues. More than 150 people have been identified by our teams, turned over to law enforcement, and subsequently arrested. This layer is invisible to the public, but don't

---

[73] In testimony before Congress, Assistant TSA Secretary Kip Hawley described it this way:

> We have deployed hundreds of BDOs at the 40 busiest airports as part of the Screening Passengers by Observation Technique (SPOT) program. The SPOT program uses nonintrusive behavior observation and analysis techniques to identify potentially high-risk passengers based solely on their exhibited behavior. BDOs are trained to detect individuals exhibiting behaviors that indicate they may be a threat. The program is a derivative of other successful behavioral analysis programs that have been employed by law enforcement and security personnel both in the U.S. and around the world.

See Kip Hawley, Assistant Sec'y, Transp. Sec. Admin., Statement Before the United States House of Representatives Committee on Transportation and Infrastructure Subcommittee on Aviation (July 24, 2008), *available at* http://www.tsa.gov/press/speeches/072408_hawley_aviation_security.shtm. Some critics are convinced that even behavior-based programs will lead to discrimination against minorities. *See generally* Herbert, *supra* note 69.

> discount it, because it may be the most effective. We publicize non-terrorist-related successes like a murder suspect caught in Minneapolis and a bank robber caught in Philadelphia.
>
> Most common are people showing phony documents, but we have even picked out undercover operatives—including our own. One individual, identified by a TSO in late May and not allowed to fly, was killed in a police shoot-out five days later. Additionally, several individuals have been of interest from the counter-terrorism perspective. With just this limited deployment of Behavior Detection Officers (BDOs), we have identified more people of counterterrorism interest than all the people combined caught with prohibited items. Look for us to continue to look at ways that highlight problem people rather than just problem objects.[74]

TSA is not alone. The techniques adopted by the agency are based on the experiences of other law enforcement agencies.[75] As the agencies and agents talk to each other, the science of facial expression will inevitably work its way into the courtroom. Collectively, society will have to answer some new questions: What weight should courts give to the new training in the context of reasonable and articulable suspicion? How do we as society want police to react under the circumstances outlined above? What are the risks to permitting the police to rely on this newly articulated way of explaining their "street sense"? What are the risks if we fail to do so?

III. SOME HIDDEN FLAWS OF THE *TERRY* PARADIGM

Psychological research suggests some additional problems that are inherent in the current paradigm. First, psychologists who study the nature of expert decision-making suggest that police officers may not be fully aware of much of the information on which they rely at the time they are using it.[76] Second, research into the nature of memory itself suggests that by requiring officers to write reports and prepare testimony to match a particular standard, the system may be irrevocably tampering with the officers' memory.[77] I consider each of these claims in turn.

---

[74] Interview by Bruce Schneier with Kip Hawley, Assistant Sec'y, Transp. Sec. Admin. (July 30, 2007), *available at* http://www.schneier.com/interview-hawley.html.

[75] *See* Burns, *supra* note 63 (noting that Ekman had previously worked with Customs and Border Protection, the Central Intelligence Agency, the Federal Bureau of Investigation, and other government agencies).

A. Naturalistic Decision Making

At least some of the dissatisfaction with the *Terry* standard on the law enforcement side is based on a fundamental mismatch between the way emergency responders, such as police officers, and lawyers think. It seems unlikely the *Terry* standard adequately reflects the reality of the practice of experienced police officers. Research into the way experts perform their jobs in other disciplines that require rapid reaction to changing circumstances in a stress-filled environment—firefighters, military officers, and jet pilots—has shown that decisions like these are not the product of the type of analysis in which judges and lawyers routinely engage.[78] Simply put, the officer on the street is engaged in a different kind of thinking than a judge on the bench.

Naturalistic Decision Making (NDM) is the term for a new field of applied psychological research. NDM "seeks explicitly to understand how people handle complex tasks and environments. Instead of trying to reduce these to variables that can be studied at leisure, NDM examines the phenomena themselves in the context of the situations where they are found . . . ."[79]

---

[76] Anthony J. Pinizzotto et al., *Intuitive Policing: Emotional/Rational Decision-Making in Law Enforcement*, 73 FBI L. ENFORCEMENT BULL., 1, 2-3 (Feb. 2004).

[77] *Cf.* Bennett L. Gershman, *Witness Coaching by Prosecutors*, 23 CARDOZO L. REV. 829, 839 (2002) ("Whereas witness preparation certainly can assist a witness in remembering and retrieving a truthful recollection, preparation can also distort a witness's underlying memory and produce a false recollection.").

[78] *See* Gary Klein et al., *Rapid Decision-Making on the Fire Ground: The Original Study Plus a Postscript*, *in* PROCEEDINGS OF THE HUMAN FACTORS SOCIETY 30TH ANNUAL MEETING 576 (1986) (firefighters); George L. Kaempf et al., *Decision-Making in Complex Naval Command-and-Control Environments*, 38 HUMAN FACTORS 220 (1996) (naval officers); PETER A. SIMPSON, NATURALISTIC DECISION MAKING IN AVIATION ENVIRONMENTS (2001), *available at* http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/3813/1/DSTO-GD-0279%20PR.pdf (jet pilots).

[79] Eduardo Salas and Gary Klein, *Expertise and Naturalistic Decision Making: An Overview*, *in* LINKING EXPERTISE AND NATURALISTIC DECISION MAKING 3 (2001).

Decision researchers such as Gary Klein, Roberta Calderwood, and Anne Clinton-Cirocco call the process that experts acting in these stressful conditions engage in "recognition-primed decisionmaking."[80] In these situations, experts do not carefully choose among a series of generated alternatives. Instead, they rapidly pattern match, looking for an experience that fits the situation.[81] We may be missing the big picture altogether by requiring explicit knowledge as the basis for a constitutional stop. According to Klein:

> Many researchers are now advocating for a dual-system mode of thinking. The automatic system is fast, automatic, effortless and emotional, and uses tacit knowledge. The reflective system is slower, conscious, effortful, deliberate, logical and serial, and uses explicit knowledge. These two systems, which work in different ways, complement each other . . . ." [82]

And these two systems do not easily connect to each other.[83] It is not hard to imagine that they also reflect the difference between the systems that take precedence for a police officer on the street, deciding whether he or the public is at risk, and for a prosecutor or judge in the office trying to decide whether that decision meets the *Terry* standard.

Return to the hypothetical officer observing the suspect on the street. Imagine that instead of the officer observing everything, a camera worn by the officer records it. The same information that was available to the camera is now available to his supervisor, the prosecutor, the judge, and ultimately the jury. Ironically, much of the information that they will be processing may not be available to the officer, at least not consciously. While he is on the street, in the danger zone, if his instincts suggest something is wrong, and that the suspect may be dangerous, his focus may change. Instead of closely watching the suspect's face, at least consciously, his focus may change to the suspect's hands and to the clothing where weapons may be hidden. His subconscious mind may be processing all of the details that we are watching on camera, but his attention is focused down on only a few things. This attention limitation may mean that, at times, the officer will have less accessible to him than we might expect when he is called upon to testify in court about the basis of his actions.[84]

---

[80] Klein, *supra* note 78.

[81] *Id.*

[82] GARY KLEIN, STREETLIGHTS AND SHADOWS: SEARCHING FOR THE KEYS TO ADAPTIVE DECISION MAKING 93 (2009).

[83] *Id.*

B. Constructed Memory and Verbal Overshadowing: Going From That's How It Must Have Happened to That's How It Did Happen

Constructed memory is one of the concerns that attorneys must grapple with for all witnesses.[85] Memory is not a fixed point, and it is constructed, and reconstructed, from the moment of the event to the moment of recall on the witness stand. Many readers of this Article have a memory of themselves involved in some significant event—a birthday party, Christmas, a wedding—where they can see themselves engaged in the activity in their mind's eye. This third-person view of the event is both real and an artifact. Barring an out-of-body experience, it is unlikely that the person with such a memory truly saw themselves that way. The image may well come from a photograph, or a video, or some other reconstruction based on family stories, fragmentary memories, and the rest of the memory is filled in around it. It may contain many important and accurate details, such as who was present, what was received, how one felt, but the image has become part of the memory in such a way that it is intertwined in one's mind.[86]

Advances in memory research show that there are multiple paths in which a witness can develop a real but false memory.[87] Factors such as stress and gap-filling can affect the acquisition of information.[88] Stress and the post-event misinformation effect can also alter memories after they have been initially encoded, and memories can be significantly affected by the passage of time.[89]

---

[84] See *infra* notes 113-19 and accompanying text for a discussion of replacing the hypothetical camera with a real one.

[85] *See* Gary L. Wells & Elizabeth F. Loftus, *Eyewitness Memory for People and Events*, *in* 11 HANDBOOK OF PSYCHOLOGY: FORENSIC PSYCHOLOGY 149, 150 (Alan M. Goldstein ed., 2003).

[86] *See* Elizabeth F. Loftus, *Memory Faults and Fixes*, 18 ISSUES IN SCI. & TECH. 42 (2002).

[87] FREDERICK CHARLES BARTLETT, REMEMBERING: A STUDY IN EXPERIMENTAL AND SOCIAL PSYCHOLOGY (Cambridge Univ. Press 1997); ELIZABETH LOFTUS & KATHERINE KETCHAM, THE MYTH OF REPRESSED MEMORY (1994).

"People integrate new materials into their memory, modifying what they believe they personally experienced. When people combine information gathered at the time of an actual experience with information acquired later, they form a smooth and seamless memory and thereafter have great difficulty telling which facts came from which time."[90]

It gets worse. Post-event suggestion, which may include new information from other witnesses, photos, records, reports, or even leading questions, often does more than refresh and bolster a fading memory.[91] It can create entirely new, and entirely false, memories.[92] Many of the criticisms of hypnotically induced memory, for example, are based on this phenomenon.[93] Memory researchers have been able to successfully implant genuinely believed but entirely false memories, demonstrating clinically that this phenomenon exists.[94]

---

[88] Wells & Loftus, *supra* note 85, at 150.

[89] *Id.*

[90] Loftus, *supra* note 86, at 43. Legal scholars have considered the dangers in the context of all witness preparation. *See also* Mirjan Damaska, *Presentation of Evidence and Factfinding Precision*, 123 U. PA. L. REV. 1083, 1094 (1975) ("During the sessions devoted to "coaching," the future witness is likely to try to adapt himself to expectations mirrored in the interviewer's one-sided attitude. As a consequence, gaps in his memory may even unconsciously be filled out by what he thinks accords with the lawyer's expectations and are in tune with his thesis. Later, in court, these additions to memory images may appear to the witness himself as accurate reproductions of his original perceptions.").

[91] Loftus, *supra* note 86, at 43.

[92] *Id.*

[93] *See, e.g.*, Amanda J. Barnier & Kevin M. McConkey, *Reports of Real and False Memories: The Relevance of Hypnosis, Hypnotizability, and Context of Memory Test*, 101 J. ABNORMAL PSYCHOL. 521, 521-27 (1992) (comparing studies of the factors affecting false memory, including hypnosis).

[94] D.S. Lindsay et al., *True Photographs and False Memories*, 15 PSYCHOL. SCI. 149 (2004) (discussing implanted false memories of being hospitalized overnight for an ear infection, spilling a punch bowl on the bride's parents at a wedding, getting one's hand caught in a mousetrap, hiding the toy slime in the teacher's desk, and witnessing a demonic possession); Elizabeth Loftus & Jacqueline Pickrell, *The Formation of False Memories*, 25 PSYCHIATRIC ANNALS 720, 720-21 (1995) (experimentally implanting false memories of being lost in a shopping mall as a young child); Giuliana Mazzoni & Amina Memon, *Imagination Can Create False Autobiographical Memories*, 14 PSYCHOL. SCI. 186 (2003).

Moreover, witness confidence in the quality of the memory can increase as the officer prepares for trial, even as the contamination increases.[95] According to experimental research done to test the effects that witness preparation had on witness confidence:

> Postevent questioning led to significantly higher later confidence ratings for incorrect responses in all three experiments, as well as for correct responses in one of the experiments. This finding is consistent with some anecdotal evidence from the legal arena that eyewitnesses often become more confident in their memories of a criminal episode as the time for testimony at trial draws near (and as the accumulated amount of postevent questioning increases).[96]

This matters in the *Terry* context because honest officers trying to recall what happened are just as likely as other witnesses to experience all of these memory-altering effects. And because they may have been involved in hundreds of similar situations by the time they testify in court, the details of one may be blurring into another. As repeat players, officers may be more, not less, susceptible to the creation of false memories.[97] An officer who has made fifty additional traffic stops in the same stretch of highway or has had fifty citizen encounters in the same area of his beat between the time he encountered a particular defendant and the time he testifies, may be unable to keep the details from blending. As the following section explains, asking him to reduce the experience to a written report, one that focuses on legally relevant facts, may preserve information, but may also have the additional effect of changing the way his memory works altogether.[98]

---

[95] *See* Steven Penrod & Brian Cutler, *Witness Confidence and Witness Accuracy: Assessing Their Forensic Relation*, 1 PSYCHOL. PUB. POL'Y & L. 817, 822 (1995) (noting that studies indicate that "confidence in one's ability to make a correct identification is a poor predictor of identification accuracy").

[96] John S. Shaw III & Kimberley A. McClure, *Repeated Postevent Questioning Can Lead to Elevated Levels of Eyewitness Confidence*, 20 LAW & HUM. BEHAV. 629 (1996).

[97] It is possible, of course, for police officers to lie, and for judges to fail to critically examine their testimony. *See, e.g.*, Laurie L. Levenson, *Unnerving the Judges: Judicial Responsibility for the Rampart Scandal*, 34 LOY. L.A. L. REV. 787, 790-91 (2001) (asserting that judges sometimes "ignor[e] telltale signs that police officers fabricate testimony to obtain convictions. . . . include[ing] amazingly similar stories by officers regarding the conduct of unrelated defendants, inconsistencies in police officer reports, [and] dramatic recalls of memory . . . .") (alteration in original).

The courts' preference for articulable experiences, and the practical support systems that come with that in the form of written reports, may actually be altering the memories of officers and witnesses over multiple stages. Translating a largely subconscious experience into *Terry* terms requires officers to go from recall of the event as a set of subjective experiences—sights, sounds, smells—to a set of verbalized experiences. By requiring officers to translate their conduct into articulable suspicion to meet the standard, we may have the unintended effect of reprogramming their memories of the event so that the standard we ask them to articulate actually alters the memory of the event to conform with the criteria.

In particular, the research of psychiatrist Jonathan Schooler has shown that using words to describe memories can interfere with recall of faces or images.[99] His work shows that recall favors the verbal description, however inaccurate it may have been initially, once the subject has committed to it.[100] Verbal memory operates through a different area of the brain than visual memory.[101] Schooler's work has shown that committing to a verbal description actually changes the part of the brain that is accessed when recalling the event.[102]

---

[98] Tanja Rapus Benton et al., *Eyewitness Memory Is Still Not Common Sense: Comparing Jurors, Judges and Law Enforcement to Eyewitness Experts*, 20 APPLIED COGNITIVE PSYCHOL. 115 (2006); Richard A. Wise & Martin A. Safer, *What U.S. Judges Know and Believe About Eyewitness Testimony*, 18 APPLIED COGNITIVE PSYCHOL. 427 (2004); *see also* C. A. Elizabeth Luuss & Gary Wells, *The Malleability of Eyewitness Confidence: Co-Witness and Perseverance Effects*, 79 J. APPLIED PSYCHOL. 714 (1994); John S. Shaw, *Increases in Eyewitness Confidence Resulting from Postevent Questioning*, 2 J. EXPERIMENTAL PSYCHOL.: APPLIED 126-46 (1996).

[99] *See* Jonathan W. Schooler and Tonya Y. Engstler-Schooler, *Verbal Overshadowing of Visual Memories: Some Things are Better Left Unsaid*, 22 COGNITIVE PSYCHOL. 36 (1990).

[100] *Id.* at 37-38.

[101] *See* Jonathan W. Schooler, *Verbalization Produces a Transfer Inappropriate Processing Shift*, APPLIED COGNITIVE PSYCHOL. 989, 992 (2002).

[102] *Id.*

IV. WHAT POLICY IMPLICATIONS SHOULD WE DRAW FROM THESE INSIGHTS?

Requiring "articulable suspicion" rather than an "inchoate hunch" may seem perfectly sensible to lawyers and judges—after all articulating is what they do.[103] Do the courts mean that the articulation should arise before the officer acts? The answer is clearly no, although that would be the time most likely to regulate police conduct. The courts have decided that the inquiry is objective, not subjective, and that while the information must have been available to the officer at the time of the event, it need not have been processed by the particular officer as such. The question is not what this particular officer thought at the time. Rather, it is what a reasonable police officer using the information available at the time might have done.

This objective approach leads to a host of concerns about the process of translating an experience in the field into testimony. For example, when and how does the officer learn and formulate the information? Can a sergeant or a supervisor help the officer to prepare? Can departments create and use question-driven report processing that drives the officer toward meeting the legal standard? Is this simply careful capturing of information, or does framing the report to meet the anticipated constitutional objections amount to impermissible witness coaching? Is it okay for the articulation to be the result of a searching inquiry by the prosecutor before the officer takes the stand? Can a prosecutor explain the rules and ask the officer to reframe his observations in a format recognizable to the courts? And how much will the process of meeting the *Terry* standard contaminate the officer's memory of the experience itself? Scholars such as Christopher Slobogin have written extensively on whether current Fourth Amendment doctrine and the exclusionary rule create incentives for officers to lie.[104] But lying, in the latter context, means that the officer is testifying in deliberate disregard for the truth; the officer has a true memory of the event, which he then disregards while testifying, in favor of a false account that will permit the officer to meet the constitutional standard.

---

[103] *See* Lerner, *supra* note 40, at 29-31 (arguing that courts privilege articulate explanations over mere hunches, often to the detriment of the search for truth).

[104] Some critics suggest that the officer is "testilying" when they alter their statements to conform with the requirements of reasonable suspicion or probable cause. Christopher Slobogin, *Testilying: Police Perjury and What to Do About It*, 67 U. COLO. L. REV. 1037, 1043 (1996).

The contaminating effects of preparing to testify can also have a truth-distorting effect, even for honest officers and prosecutors. We should ask applied cognitive psychologists to study whether current Fourth Amendment doctrine and the mechanisms we have created to enforce it are causing officers to give subjectively true testimony regarding their encounters, i.e., statements that reflect their memory as they perceive it, but that have been altered by the process of capturing and accessing the information in constitutional terms. Specifically, the existing research begs us to consider how much the inquiry that prosecutors go through when preparing the witness, or even a witness's anticipation of the line of questioning, alters the way the police officer remembers the event.[105] Given that words and experiences often reside in different parts of the brain itself, does the process of writing a police report fundamentally alter the nature of the memory itself? Is a form that directs thinking down certain paths, or training that directs officers to remember things in certain, court-approved ways, changing the nature of the experience itself? Given that memory is constructed, does the way we apply the standard help or hurt the courts in their quest for accuracy?[106]

Once we have some answers from the applied psychologists, attorneys and the courts have a related set of questions to examine. How does the administrative decision to adopt these methods and train law enforcement to deploy them factor into Fourth Amendment reasonableness? Is there some deference due to the executive branch in this area?[107] How sure do the courts have to be that the officer was wrong to suppress? How should the burdens be allocated—legally and in reality? Are there technological solutions that can help us sort through these problems?

---

[105] For a review of the risks, see generally Fred C. Zacharias & Shaun Martin, *Coaching Witnesses*, 87 KY. L.J. 1001 (1999); Joseph D. Piorkowski, Jr., *Professional Conduct and the Preparation of Witnesses for Trial: Defining the Acceptable Limitations of 'Coaching,'* 1 GEO. J. LEGAL ETHICS 389 (1988); and Gershman, *supra* note 77.

[106] While this Article is focused on the *Terry* inquiries, the same questions apply to preparation based on the elements of an offense. If one spends enough time in traffic court, one will hear the almost liturgical repetition of the factors that led an officer to administer a breathalyzer or equivalent blood alcohol test. It goes something like this: "I approached the vehicle and examined the subject. There was a strong odor of alcohol. The subject's eyes were glassy and bloodshot. His speech was slurred and his response to questions was delayed, and he appeared confused. Based on these preliminary indicators, I chose to administer a field sobriety test, (and a field test for blood alcohol if appropriate in the jurisdiction), and then placed the subject under arrest, before transporting him to the station for the administration of a BAC test under controlled conditions." I have personally seen officers give this speech, or a very close variant of it, on more than a dozen occasions over the course of a single day in traffic court.

Other observers of the *Terry* regime are comforted by the idea that even inefficient and dysfunctional judicial oversight is better than no oversight. Some have gone so far as to label *Terry* a "practically perfect" doctrine.[108] How much comfort should we take if the costs are fully on the table? Has the Court stunted the development of alternative methods of policing the police by creating a false sense that there is someone watching the watchers?[109]

A. Enforcement of the Standard

Courts enforce the Fourth Amendment through the exclusionary rule. And they have chosen to do so through a standard that reflects the courtroom's inherent bias in language skill. But while the courts will suppress evidence, they are loath to find an officer to have deliberately lied. It does evoke the question: How do we tell the honest but inarticulate officer from the corrupt officer? One way to interpret the deference that underlies many of the opinions and practices is that the courts have a sense that most police officers are doing a trying and dangerous job, that it is experiential, and that it may be hard to translate those experiences into words. And the courts assume that most of the time the officers are acting in good faith. It seems at least possible that the reluctance to punish police officers for Fourth Amendment violations stems in part from a tacit realization that there are genuine but inarticulable experiences that at least some of these police officers have relied upon to conduct what would otherwise appear to be violative stops. That is, good cops, with good street sense, have been bad at explaining why they were doing what they were doing.[110] Judges implicitly recognize the memory contamination effects and the differential language skills of officers when they find an officer has testified incorrectly but not falsely.

---

[107] For a discussion of the deference courts show to police, see Becton, *supra* note 41, at 470-71.

[108] *See* Saltzburg, *supra* note 4.

[109] Levenson, *supra* note 97, at 790-91.

This reluctance to find that officers have lied may lead to inaction even in cases where action is warranted. In her post-mortem of the Rampart scandal in Los Angeles, where corrupt police officers were framing innocent individuals, and falsifying testimony about others, Professor Laurie Levenson noted that even conscientious judges who find an officer's testimony to be false in a particular case are unlikely to go beyond that.[111] As she put it:

> There has been a failure by judges who have witnessed police perjury to take meaningful action to prevent such misconduct in the future. A judge's standard course of action when an officer has lied is to dismiss the case or grant a motion to suppress, and ask the prosecutors to report the misconduct to appropriate police internal affairs authorities. There is no follow-up by the court, no judicial reporting of the misconduct, no contempt orders, and no tracking of the problem officers. As a result, while a judge may occasionally take an interest in a particular case, systemic problems with corrupt police officers continue. [112]

---

[110] The problem I am discussing is different from the problem addressed by scholars such as Christopher Slobogin, who suggests that current Fourth Amendment doctrine and the exclusionary rule create incentives for officers to lie, and Melanie Wilson, who is seeking ways to empirically test this proposition. *See* Slobogin, *supra* note 104, at 1041-48 (discussing the issue of false police testimony and indications that it occurs); *see also* David N. Dorfman, *Proving the Lie: Litigating Police Credibility*, 26 AM. J. CRIM. L. 455, 470-71 (1999) (noting that judicial opinions impugning the motives, honesty, or competency of police are rare); Stanley Z. Fisher, *"Just the Facts, Ma'am": Lying and the Omission of Exculpatory Evidence in Police Reports*, 28 NEW ENG. L. REV. 1, 36-38 (1993) (discussing police access to exculpatory evidence and its absence from their reports.); Melanie D. Wilson, Judging Police Lies—An Empirical Perspective (Jan. 2010) (unpublished manuscript), *available at* http://works.bepress.com/cgi/viewcontent.cgi?article=1002&context=melanie_wilson.

[111] Levenson, *supra* note 97, at 194.

[112] *Id.*

VI. CAMERAS AS A SOLUTION

As detailed above, current Fourth Amendment doctrine may actually encourage practices that restructure an honest officer's memory in unappreciated ways. Officers are witnesses, and are susceptible to the same faults of memory that apply to all eyewitnesses, including the raft of problems associated with constructed memory. Because memory is constructed, the searching inquiry that attorneys engage in when preparing or cross-examining the witness may alter irreparably the way the police officer remembers the event. Given that words and experiences often reside in different parts of the brain itself, the process of writing a police report tailored to meet Fourth Amendment demands may likewise fundamentally alter the nature of the memory itself. Report forms that direct an officer's thinking down certain paths, or training that directs officers to remember things in certain, court-approved ways, may change the nature of the experience itself because officers have their attention directed and constrained.

Given these dangers, a new approach is warranted. Reasonable and articulable suspicion, the traditional *Terry* standard, should be reframed more broadly, as reasonable suspicion supported by credible evidence. Articulable suspicion is only a subset of a larger category, based on the reasonableness more generally. The important issue is whether the courts are able to meaningfully engage in oversight of the police and remain capable of protecting the citizenry's Fourth Amendment rights. The courts should be able to make that determination based on any available evidence. Oral testimony is only one way to make the officer's action amenable to judicial review, which is the purpose of the exercise.

We are now entering the age of widespread deployment of cameras in police cars and even on police officers themselves.[113]

---

[113] Every state police agency has used some form of video recording system in patrol cars and the International Association of Chiefs of Police estimates that nearly half of police cars are equipped with a video camera. Matthew D. Thurlow, *Lights, Camera, Action: Video Cameras as Tools of Justice*, 23 J. MARSHALL J. COMPUTER & INFO. L. 771, 795 (2005). For an extensive discussion of the use of officer-mounted cameras, see David A. Harris, *How Accountability-Based Policing Can Reinforce—Or Replace—The Fourth Amendment Exclusionary Rule*, 7 OHIO ST. J. CRIM. L. 149, 175-80 (2009). Civil

Cameras are everywhere, and an increasing number of departments and prosecutors have worked through the logistics of using police cameras. With the widespread use of ever-cheaper digital video, it is now clear that the costs of deploying cameras can be managed,[114] and that protocols for handling discovery issues can be developed.[115] Given the hidden costs of the current regime, states should consider adopting policies that mandate the use of video.

One objection to the use of video is cost, but the price of the technology to capture and store video is dropping steadily and should continue to drop as more vendors enter the market.[116] Cross-adoption of technology should also help. Anyone who has purchased a smartphone in the last two years had the option of purchasing one that recorded and transmitted video clips. Once it becomes clear that there is a large enough market for a robust, officer-worn video-recording device, competitors who have developed hardware expertise in these other contexts will enter the market, driving costs down even further.

Some of the more difficult obstacles to the adoption of video remain cultural. Right now, many departments and police chiefs are comfortable with video so long as they can decide when it is used—to make cases and to protect their departments from false liability claims. But the video has the potential to act as a double-edged sword. There will be uses of police video in court not only for departments when they are falsely accused of violating a suspect's rights or as evidence against defendants, but also against the police when officers have in fact violated defendants' rights, or the

---

libertarians have not been comfortable with cameras for other reasons, so their use will remain controversial. For a discussion of the mechanics of digital camera deployment in a broader context—and a critical view of widespread use of cameras without Fourth Amendment regulation, see CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 81-110 (2007); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213 (2002); Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS. 125, 152 (2002).

[114] Thurlow, *supra* note 113, at 797.

[115] I anticipate that the cameras will produce what will be another form of digital evidence. *See generally* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279 (2005) (discussing potential protocols for managing digital evidence).

[116] Thurlow, *supra* note 113, at 797.

video is used as evidence by defense counsel in unforeseen ways.[117] Departments that resist the deployment of cameras are more worried about the perceived downside than the upside.[118]

One underexplored upside is the one this Article explores. There is plenty of doctrinal room within current Fourth Amendment jurisprudence for the use of digital video as a supplement to, or substitute for, police testimony. Using video will also allow the new science on facial expression to be considered, while subjecting it to judicial oversight, expert reexamination, and public scrutiny. Having video available will also reduce the problems with memory contamination explored above by permitting officers to examine the video before testifying and hopefully them from locking in to a verbal formulation of the event that may not reflect reality. It should also simplify life for prosecutors and defense attorneys. It will make cases based on good stops easier to prove, and bad cases easier to weed out. This rise in quality will lead to an increase in pretrial resolutions in both directions, saving trial resources for cases where there are genuine disputes.[119] Finally, video evidence will empower judges to act in cases where officers are truly lying because it will obviate the swearing contest between a police officer and an accused criminal, and give judges much firmer footing on which to stand.

---

[117] A 2004 study by the International Association of Chiefs of Police demonstrated that ninety-seven percent of U.S. citizens responding to a poll supported the use of in-car cameras for law enforcement. Colonel Thomas Hutchins, *In-Car Cameras: Executive Summary*, *in* IACP/COPS TECHNOLOGY TECHNICAL ASSISTANCE PROGRAM: TECHNOLOGY DESK REFERENCE 47 (2010) ("While law enforcement views the acquisition of camera technology as a means to demonstrate their professionalism and increase officer safety, the public views cameras as a means to guard against abuse. Despite the difference in opinions, both the public and the police support use of the technology making the acquisition and implementation of an in-car camera program a win/win proposition for all.").

[118] Of course, for outsiders, accurate assessments of officer conduct are likely to be seen as all upside, whether the camera reveals that the officer was good or bad.

[119] This article is focused on the costs and benefits of the *Terry* regime. Cameras have multiple other benefits for law enforcement. For example, they can provide clear evidence in criminal trials and civil suits, resolve disciplinary complaints against officers, allow oversight and training by supervisors, and increase public confidence that officers are accountable. For further exploration of these issues, see David Harris, *Picture This: Body Worn Video ("Head Cams") As Tools For Ensuring Fourth Amendment Compliance By Police*, 43 TEX. TECH L. REV. 357 (2010) (discussing the various contexts in which video evidence would be useful).

Whether and to what extent the evidentiary rules should *require* video before permitting certain kinds of testimony, such as the testimony on facial expression, remain open questions.

CONCLUSION

This Article has outlined some of the unexplored costs of the *Terry* regime, built on the requirement of reasonable and articulable suspicion. The current regime has flaws as practiced, and a range of challenges coming that it must face. Research on witness memory has demonstrated that there are contamination effects that are a byproduct of the way we now practice Fourth Amendment law. New pressures on the *Terry* regime are coming from other directions as well. The federal government and the police are training officers in new techniques based on advances in cognitive and behavioral science that rely on officer observation of suspect behavior, much of it subtle and operating in ways that the suspects themselves do not realize. Inevitably, officers relying on the new techniques will be bringing them into the courtroom, where the doctrine will be forced to adapt. *Terry* as now practiced may be giving us a false sense of security, while failing in two directions simultaneously. It creates the sense that the courts are meaningfully engaged in police oversight, leaving it less likely that other administrative oversight methods will be adopted. The current formulation may also be limiting perceptions about the appropriate use of evidence in some subset of cases where a good, but inarticulate officer engages in a search that we would like to take place, and has the evidence suppressed because he is inarticulate about his reasonable suspicion. Technology is also increasing the range of evidence that is available to the courts when deciding if officers acted reasonably. Rather than relying on witness testimony alone, digital video is subjecting a wide range of heretofore unavailable behavior to the courts. It is time to move beyond the *Terry* formulation of the basis for police frisks. By explicitly adopting a new standard—reasonable suspicion supported by credible evidence—the courts can make clear that there is doctrinal room for technology, in the form of cameras today and perhaps in other forms tomorrow, to help ameliorate the limitations of human memory, while allowing society the benefit of other advances in our knowledge of cognitive science.

WESTERN UNION, THE AMERICAN FEDERATION OF LABOR, GOOGLE, AND THE CHANGING FACE OF PRIVACY ADVOCATES

Wesley MacNeil Oliver[*]

INTRODUCTION 971
I. HISTORY AND EXPANSION OF TELEGRAPH COMMUNICATION 973
II. GOVERNMENT INTRUSION OF TELEGRAPH TECHNOLOGY AND SOCIETY'S REACTION..................................974
III. HISTORY AND EXPANSION OF TELEPHONE TECHNOLOGY 979
IV. GOVERNMENT INTRUSION OF TELEPHONE TECHNOLOGY AND SOCIETY'S REACTION.................................980
V. THE NEXT COMMUNICATIONS REVOLUTION 985

INTRODUCTION

Law professors fondly observe that the law is always catching up with technology. What else could it do? Legislators could hardly be expected to anticipate scientific discoveries. Technological foresight is rarely a campaign promise or the basis for selecting elected officials. Judges are rarely experts in science and engineering. Gone are the days of Benjamin Franklin, Thomas Jefferson, and Benjamin Rush, when scientists and inventors were also lawgivers.

Is there, however, something insightful we can gather from the oft-noted, and facially obvious, observation that regulation follows invention? Perhaps by looking at why earlier invention sparked regulation, we can understand whether, or how, modern invention will produce legal limits.

---

[*] Associate Professor, Widener University School of Law, J.D. University of Virginia; LL.M., J.S.D. Yale Law School.

The question has particular relevance for the rapidly emerging methods of modern communication. The recent pace of development in communication technology leaves privacy interests in the new media considerably unprotected by comparison with traditional means of communication. The government must jump over considerably more legal hurdles to listen in on telephone conversations than it does to obtain e-mails or discover where a cell phone user traveled.[1]

The gap between emerging technologies and laws protecting privacy interests in those communications is hardly new. Few technologies have seen explosions both in sophistication and widespread use as electronic communication. For America's first century, methods of communication did not change, though the speed and reliability of the ordinary mail improved substantially over the period.[2] Then, and almost overnight, communication technology took a great leap forward as telegraphs, and soon thereafter telephones, became commonplace in major cities. Roughly a century later, another revolution occurred in the way society communicates.

Lawmakers anticipated privacy concerns in e-mails, texts, and instant messages no better in the twentieth century than their counterparts in the nineteenth century. Nineteenth-century government investigators were able to obtain the contents of telegrams with simple subpoenas, subject to effectively no judicial supervision.[3] Likewise, early twentieth-century police officers were not required to receive authorization to intercept telephone calls.[4] However, the law did eventually "catch up" with technology as limits were placed on the government's ability to intercept telegraph and telephone communications.[5]

---

[1] Haley Plourde-Cole, *Back to* Katz*: Reasonable Expectations of Privacy in the Facebook Age*, 38 FORDHAM URB. L.J. 571, 589 (2010).

[2] Sharon K. Sandeen, *In for a Calf is not Always in for a Cow: An Analysis of the Constitutional Right of Anonymity as Applied to Anonymous E-Commerce*, 29 HAST. CONST. L.Q. 527, 536 n.24 (2002) (citing CARL H. SCHEELE, NEITHER SNOW NOR RAIN . . . : THE STORY OF THE UNITED STATES MAILS (1970)).

[3] *See* Wesley MacNeil Oliver, *America's First Wiretapping Controversy in Context and as Context*, 34 HAMLINE L. REV. 205, 216 (2011).

[4] *Id.* at 234-35.

[5] *Id.* at 226-31 (describing protections in telegraph communications); Neal Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA*

It is not clear that the law will do the same in the twenty-first century. Much has changed since our last communications revolution roughly a century ago. The interest groups that shaped privacy expectations after our first communications revolution are not as powerful as they were a century ago. The American Civil Liberties Union, for instance, does not have the influence organized labor had in the early twentieth century. Corporate privacy advocates have also changed. Today, they come with unclean hands. Telephone and telegraph companies argued for their customers' privacy against government intrusion.[6] Providers of modern communications services argue for their customers' privacy from the government, but while selling customers' information to advertisers for a fee.[7] The history of communication technology, and its protection from the government's prying eye, is relevant to predicting how the law will regulate recent innovations. Telegraph communications offered the first alternative to the existing and quite slow method of getting messages from one place to another. Remarkably fast Pony Express riders could get letters from St. Louis to California in eight days, beating the pace of stage coaches by twelve days. Telegrams, by contrast, permitted messages to travel thousands of miles almost instantly.

I. HISTORY AND EXPANSION OF TELEGRAPH COMMUNICATION

Samuel Morse conceived of the electromagnetic telegraph in 1832, built an experimental one in 1835, and constructed a truly practical system in 1844.[8] Telegraph technology achieved "commercial practicability" in major eastern cities between 1845

Surveillance Program: The FDR Precedent, 60 STAN. L. REV. 1023, 1041-47 (2008) (describing emerging protection of telephone privacy).

[6] *See* United States v. Babcock, 24 F. Cas. 908 (E.D. Mo. 1876) (first of a number of cases in which Western Union challenged a subpoena for disclosure of the contents of telegrams); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 598 (2009) (describing amicus brief of telephone companies in *Olmstead v. United States*, 277 U.S. 438 (1928)).

[7] *See* Cade Schmidt, *Google Doesn't Do Data Mining; Er, Is That a Joke Too?*, REGISTER (Sept. 23, 2010), http://www.theregister.co.uk/2010/09/23/schmidt_on_colbert/.

[8] *The Morse Telegraph*, HISTORY WIRED: A FEW OF OUR FAVORITE THINGS, http://www.historywired.si.edu/object.cfm?ID=306 (last visited Jan. 21, 2012).

and 1846.[9] Messages could be conveyed across the Atlantic Ocean by this device by 1858.[10] Telegraph messages, however, remained a tool for commercial transactions or highly important personal communications as these messages were billed at high rates by the syllable.[11] These messages were also, by definition, less than completely private. Regardless of any laws designed to ensure privacy of the customer's messages, it was inevitable that at least the operator and transcriber would know the contents.[12]

With the invention and widespread use of telegraph and telephone technology, it was initially assumed that the government had complete access to any message passed across these media. The sender revealed the contents of his message to a third party, the telegraph or telephone carrier, and thus lost his expectation of privacy in the message—at least he lost his expectation from government intrusion. High profile government intrusions on these forms of communication outraged the providers of these new forms of technology, as well as their customers, who had reason to fear that sensitive information might be intercepted.

II. GOVERNMENT INTRUSION OF TELEGRAPH TECHNOLOGY AND SOCIETY'S REACTION

Though telegraph technology was available from the mid-nineteenth century, it was expensive and rarely used. The Civil War awakened potential customers to the value of instantaneous communications. Military commanders used the wires to transmit orders and reporters used the wires to relay news.[13] Civilian use of telegraphs increased dramatically after the war.[14]

---

[9] Richard B. DuBoff, *Business Demands and the Development of the Telegraph in the U.S., 1844 to 1860*, 54 BUS. HIST. REV. 459 (1980).

[10] This system, however, broke down after two works of operation and would only be restored after the Civil War. RICHARD F. SEKER, CIVIL WAR AMERICA 58 (2006).

[11] Oliver, *supra* note 3, at 234.

[12] *See* Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 577-78 (2007).

[13] LEWIS COE, THE TELEGRAPH: A HISTORY OF MORSE'S INVENTION AND ITS PREDECESSORS IN THE UNITED STATES 51-65 (2003).

[14] Richard R. John, *Recasting the Information Infrastructure for the Industrial Age*, *in* A NATION TRANSFORMED BY INFORMATION: HOW INFORMATION HAS SHAPED THE UNITED STATES FROM COLONIAL TIMES TO THE PRESENT 55, 81 (Alfred D. Chandler, Jr. & James W. Cortada eds., 2000); U.S. CONG., REPORT ON POSTAL TELEGRAPH 10 (1884).

The value of eavesdropping on this method of communication that came of age during the war was also quite apparent. Intercepting military messages became a matter of deadly sport. For obvious reasons, there was no expectation of privacy in these communications. Messages were sent in code because of the high likelihood of interception.[15] The coded messages were often published in newspapers where the public's assistance in deciphering these messages was sought.[16]

After the war, government investigators quickly discovered the value of the medium that required information to be disclosed by the sender to the telegraph company. With the end of the hostilities, they did not have to be as crafty as the military spies who intercepted telegraphs. Permanent records of messages remained in the possession of telegraph companies.[17] Investigators merely had to obtain access to these records to determine messages had been exchanged.

Investigations early in the telegraph era revealed that telegraph customers had considerably less expectations of privacy than postal customers. Some of these investigations were very low-tech. During the impeachment proceedings against President Andrew Johnson, Congressman Benjamin Butler sent private detectives to indiscriminately seize copies of thousand of telegrams passing in or out the telegraph offices in Washington and Baltimore.[18] Some of the telegrams were seized to substantiate the charges against Johnson.[19] Following his acquittal, Butler used the telegrams to support his claims that Kansas Senator Edmund Ross had been bribed to vote for acquittal.[20]

---

[15] DAVID HOMER BATES, LINCOLN IN THE TELEGRAPH OFFICE 49-67 (Univ. of Neb. Press 1995) (1907).

[16] TOM WHEELER, MR. LINCOLN'S T-MAILS: THE UNTOLD STORY OF HOW ABRAHAM LINCOLN USED THE TELEGRAPH TO WIN THE WAR 100 (2006).

[17] 1855 Pa. Laws 531 (requiring telegraph operators "to preserve the originals of all [telegraph] messages sent from such office . . . for at least three years . . . ."); *see generally* MORRIS GRAY, A TREATISE ON COMMUNICATIONS BY TELEGRAPH 115 (1885) (explaining the rights of action against telegraph companies because in order to be criminally liable under the statute there must be a right of action).

[18] DAVID J. SEIP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 30 (1978).

[19] *Id.*

[20] *Id.* at 31.

Government investigators after the impeachment did not rely on such thuggish tactics to obtain telegrams. A subpoena *duces tecum* for telegrams provided the imprimatur of judicial authorization without any meaningful oversight of a court. Most states had statutes forbidding a telegraph company from disclosing the contents of a message to anyone but the intended recipient, but the statutes, on their face, largely left unclear whether these messages could be disclosed to criminal investigators or courts.[21] Courts never construed these statutes to limit the scope of the subpoena power.

The use of a subpoena, as opposed to Benjamin Butler's methods, provided the nation's primary telegraph company an opportunity to object to the seizure of copies of telegrams before the fact. The first high-profile objection to complying with a subpoena for telegrams involved an allegation of political corruption. Federal prosecutors suspected that President Ulysses S. Grant's personal secretary, Orville Babcock, was tipping off St. Louis distilleries about raids to discover tax evasion.[22] They obtained a subpoena for all the telegrams sent between Grant's secretary and a revenue agent in St. Louis for an eight-month period.[23] In modern criminal cases, we are accustomed to the defendant seeking to prevent the prosecution from using evidence on the basis that his privacy rights have been intruded upon.[24] In these early telegraph subpoena cases, the telegraph company itself objected to producing information that could be used to incriminate its clients.

---

[21] *See* HENRY HITCHCOCK, INVIOLABILITY OF TELEGRAMS: A PAPER READ AT THE SECOND ANNUAL MEETING OF THE AMERICAN BAR ASSOCIATION 26 (1879) (observing that only Missouri and Indiana had laws prohibiting telegraph operators to divulge the contents of telegrams but expressly provided an exception when the information was requested by a court). Hitchcock's otherwise excellent research appears to have omitted at least one state, Pennsylvania, which had a similar exception. 1855 Pa. Laws 531.

[22] ROY MORRIS, JR., FRAUD OF THE CENTURY: RUTHERFORD B. HAYES, SAMUEL TILDEN, AND THE STOLEN ELECTION OF 1876 at 25-26 (2003).

[23] United States v. Babcock, 24 F. Cas. 908 (E.D. Mo. 1876).

[24] In fact, in the modern era the telegraph company would lack standing to object to even an illegal search that produced evidence against one of its customers. *See* United States v. Payner, 447 U.S. 727, 732 (1980) (even egregious trespass upon privacy and property interests of bank's employee does not provide remedy for bank's customer); *see also* Jerry E. Norton, *The Exclusionary Rule Reconsidered: Restoring the Status Quo Ante*, 33 WAKE FOREST L. REV. 261, 296-97 (1998) (criticizing *Payner* and three other cases that established a standing rule permitting the exclusionary rule to apply "only [to] the person whose Fourth amendment right" was disregarded).

Western Union, obviously attempting to assure its customers their privacy would be protected, objected to such a sweeping request for telegrams.[25] The telegraph company argued that the government had not shown the information they sought could be found within these documents. Their arguments dealt both with the degree of suspicion required to obtain the documents and the amount of specificity required of the request.[26] A vast amount of their customers' private communications would be delivered to the government with such requests. The federal court rejected Western Union's concern, requiring only that subpoenas identify needed telegrams "with that degree of certainty that is practicable[;]" a criterion the court found satisfied by the government's request in this case.[27]

Three years later, a congressional committee investigating the Presidential Election of 1876 issued subpoenas for an untold number of telegrams identified only by parties and a wide range of dates.[28] With the election too close to call, and allegations of fraud and voter intimidation in Florida, Louisiana, and South Carolina, a congressional committee subpoenaed—among others things—all telegrams sent to or from eight prominent Louisiana Republicans, all suspected of involvement in voter fraud. The subpoenas for these men covered a four-month period.[29]

As it had done in the *Babcock* case, Western Union opposed the subpoenas for the telegrams. The testimony of the telegraph operator assigned to the New Orleans office was read before the congressional committee:

> I am instructed that a judicial or other *subpoena* couched in such general and sweeping terms would be in legal effect a *general warrant*, within the prohibition of the fourth amendment to the Constitution of the United States, and subject to the condemnation of the great

---

[25] Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892, 1901 (1981).

[26] Oliver, *supra* note 3, at 221-22.

[27] *Babcock*, 24 F. Cas. at 909.

[28] 44 CONG. REC. H452 (daily ed. Jan. 5, 1877).

[29] *Id.*; MORRIS, *supra* note 22, at 175-85, 192-99, 203.

> principles of personal liberty and private right established for all freemen of the Anglo-Saxon race by the celebrated judgments of Lord Camden in Wilkes's case, and the case of *Entick v. Carrington* . . . .[30]

The committee rejected Western Union's argument, concluding that customers' privacy interest in the contents of telegrams did not defeat the superior interest of the government in discovering information.[31] The committee further rejected the analogy to general warrants.[32] The subpoena itself was beyond constitutional challenge, according to the committee's reasoning: "[I]n the hundreds of instances in which the *subpoena duces tecum* has been resorted to . . . the similarity which the witness supposes to exist between that writ and the 'general warrants' condemned by the constitutional provision cited by him has never yet been detected."[33] Of course, it was not the subpoena itself, but the use made of the subpoena, that Western Union claimed amounted to an indiscriminate search forbidden by the Constitution.[34]

Western Union continued to argue against requests for all telegraph communications passing between identified persons.[35] In 1878, a state grand jury in St. Louis issued a subpoena for all the telegrams sent between four named persons over a fifteen-month period.[36] Western Union objected that such requests violated the federal and Missouri Constitutions' prohibition on unreasonable searches and seizures.[37] This time, the Missouri Supreme Court, in *Ex Parte Brown*, accepted Western Union's position.[38] The court concluded that Missouri's constitutional prohibition on unreasonable searches and seizures required that a subpoena:

> [S]hall at least give a reasonably accurate description of the paper wanted, either by its date, title, substance, or

---

[30] 44 CONG. REC. H454 (daily ed. Jan. 5, 1877).

[31] 44 CONG. REC. H603 (daily ed. Jan. 12, 1877).

[32] *Id.* at 603-04.

[33] *Id.* at 604.

[34] *Id.* at 603.

[35] *Id.* at 604.

[36] *Ex Parte* Brown, 72 Mo. 83, 90 (Mo. 1880).

[37] *Id.*

[38] *Id.* at 93.

> the subject it relates to . . . . To permit an indiscriminate search among the papers in one's possession for no particular paper, but some paper, which may throw some light on some issue involved in the trial of some cause pending, would lead to consequences that can be contemplated only with horror, and such a process is not to be tolerated among a free people.[39]

The *Brown* particularity requirement, zealously advocated for by Western Union in a variety of settings, became the standard for telegram subpoenas throughout the nation.[40] The telegraph company's continued zealous advocacy led courts to fashion some protections from the government's ability to know the content of all telegraphed communications.

III. History and Expansion of Telephone Technology

One might imagine that late-nineteenth-century legislatures anticipated the possibility (or probability) that government investigators would have a similar interest in discovering the contents of telephone calls. Yet laws meaningfully protecting privacy in telephone conversations did not accompany this innovation in communication technology.

The telephone, just a few decades behind the telegraph, both in invention and widespread availability, gave ordinary Americans access to immediate communications. Alexander Graham Bell's telephone was first displayed at the 1876 World's Fair in Philadelphia.[41] Two years later, the first telephone exchange opened in New Haven, Connecticut, and within a few years, telephone service was available in every major city in the country.[42] Customers were much more willing to use telephones to communicate than telegraphs.[43] Initially, subscribers were permitted unlimited use to encourage them to transfer to this method of communication from the telegraph service that billed by the message.[44] By the 1890s, callers paid for the amount of their individual usage.[45]

---

[39] *Id.* at 94.

[40] *See* Desai, *supra* note 12, at 582 (observing that after *Brown*, courts generally required specificity in warrants analogous to that required by the Missouri Supreme Court). While the United States Supreme Court recognized in *Boyd v. United States*, 116 U.S. 616, 633 (1886), that the Fourth Amendment protected citizens from subpoenas for the production of their documents, subpoenas for telegraphed messages continued as those holding the records of those messages, either custodians of corporate records or telegraph offices, had no privacy or property interests in the contents of the messages. *See* Wheeler v. United States, 226 U.S. 478, 488 (1913); Wilson v. United States, 221 U.S. 361 (1911); *Ex Parte* Gould, 132 S.W. 364, 374-80 (Tex. Crim. App. 1910).

[41] CHERYL GANZ, THE 1933 CHICAGO WORLD'S FAIR: CENTURY OF PROGRESS 79 (2008).

Telephone conversations provided an immediate response, unlike the telegraph which required a chain of delivery and a wait period for a response. Telephones, at the turn of the twentieth century, had made instantaneous communications accessible to the masses.[46]

IV. GOVERNMENT INTRUSION OF TELEPHONE TECHNOLOGY AND SOCIETY'S REACTION

Laws written to ensure privacy in telegraphs were poorly adapted to account for the new technology of the telephone. In New York, for instance, statutory provisions prohibited interception of telegraphs and forbad telegraph companies from disclosing the contents of a telegram to anyone but the intended recipient.[47] Telegraph companies were also forbidden to send messages that constituted or furthered a crime and were required to forward such messages to law enforcement authorities. With the development of telephone technology, the legislature simply added the words "or telephone" and "telegraph."[48] While it was theoretically possible for telegraph operators to identify criminal messages before sending them, it was simply not possible with the telephone. Late nineteenth-century lawmakers lacked even this basic insight and had not learned other—more subtle—lessons from investigations involving telegrams. It should have been foreseeable that law enforcement would have an interest in learning the contents of telephone conversations, just as it had an interest in discovering the contents of telegrams. The laws nevertheless forbid any interception, whether by law enforcement or others.

---

[42] JOHN E. KINGSBURY, THE TELEPHONE AND TELEPHONE EXCHANGES: THEIR INVENTION AND DEVELOPMENT 267 (1915).

[43] *Id.* at 473.

[44] *Id.*

[45] *Id.*; *see also* MORRIS, *supra* note 22, at 23 (explaining that prepaid message requirements were likely to be considered a reasonable telegraph company regulation).

[46] *See* AMERICAN TELEPHONE AND TELEGRAPH COMPANY, TELEPHONE STATISTICS OF THE WORLD 8-13 (1912) (describing that telephone use in the first decade of the twentieth century increased nearly ten times more rapidly than telegraph use).

[47] *See* N.Y. PENAL LAW § 641 (McKinney 1881).

[48] 1895 N.Y. Laws 518 (current version at N.Y. PENAL LAW § 250.35(1) (McKinney 2008)).

Despite these laws, just as with telegraph technology, government officials initially assumed there were no limits on their ability to intercept conversations passed along the wires. The New York City Police Department maintained a wiretap squad from 1895 that operated in secret.[49] None of the evidence it obtained was ever introduced in court. Information obtained from the wiretaps was used only to aid in investigations, which kept the program from ever coming to light.[50]

A high-profile dispute in 1916 between the mayor of New York and the Catholic charities of New York ended the secrecy of what appears to have been this country's first wiretapping program.[51] In an effort to demonstrate that priests were attempting to avoid testifying before a committee investigating their use of city funds, Mayor John Purroy Mitchel ordered the police department to intercept the calls of priests who were to testify.[52] A Catholic member of the wiretap squad, having second thoughts about eavesdropping on a priest, revealed the mayor's actions and thus the existence of the entire wiretapping program.[53]

---

[49] *Seymour Wires Tapped on Order Given By Woods*, N.Y. TIMES, May 18, 1916, at 1 ("The practice of wiretapping . . . goes back as far as 1895 . . . . The company . . . interpreted the law to mean that it was its duty to aid and assist the public officials in apprehending and detecting crime . . . ." (quoting John L. Swayze, general counsel of the New York Telephone Company)).

[50] STATE OF NEW YORK, MINUTES AND TESTIMONY OF THE JOINT LEGISLATIVE COMMITTEE APPOINTED TO INVESTIGATE THE PUBLIC SERVICE COMMISSIONS 103 (1916) (testimony of Police Commissioner Arthur Woods), *available at* http://www.archive.org/stream/cu31924083762942#page/n15/mode/2up.

[51] *See* EDWIN R. LEWINSON & JOHN PURROY MITCHEL: THE BOY MAYOR OF NEW YORK 179-80 (1965); Meyer Berger, *Tapping the Wires*, NEW YORKER, June 18, 1938, at 41.

[52] Daniel Trucano, The Public Charities Controversy and John Purroy Mitchel, Mayor of New York City, 1914-17 (Apr. 10, 1970) (unpublished master's thesis, St. Francis College) (on file with author).

The disclosure of the previously secret police wiretap squad attracted considerable public attention.[54] There was an immediate fear that every New Yorker's telephone conversations were being overheard. The police were able to convince the public that they were sufficiently competent at investigation and that the phones of few, if any, innocent persons were ever tapped.[55] Police Commissioner Arthur Woods explained that the New York City police were not the bumbling constables Benjamin Cardozo described from the Framing Era.[56] He explained that his professional police department had expertise in identifying criminals and was rarely wrong when it engaged in an intrusion as serious as a wiretap.[57]

For the most part, Police Commissioner Woods's claim that the New York Police Department should be trusted to determine who to wiretap seemed to satisfy New Yorkers.[58] Charges against city officials for conducting the wiretapping were dropped.[59] Though laws were proposed in the legislature that year to limit the ability of police to decide when to eavesdrop on telephone calls, none passed.[60] The mayor who ran against Mitchel's clearly politically motivated wiretapping implemented only modest reform. Under his administration, police only had to obtain the approval of a prosecutor to conduct requested wiretapping.[61] Self-regulation of wiretapping thus appears to have been largely in the

---

[53] Michael W. Clark, Mayor Mitchel, Wire-Tapping, and the Catholic Vote of 1917 in New York City 28-29 (1965) (unpublished master's thesis, St. Francis College) (on file with author).

[54] *See* Oliver, *supra* note 3, at 239 n.207.

[55] *Id.*

[56] *See* People v. Defore, 150 N.E. 585, 587 (N.Y. 1926). Of course police in the 1920s were not the constables of the Framing Era. They were considerably more powerful, with considerably more power and incentive to consciously disregard civil liberties than the colonial-era title constable suggested. *See* Wesley MacNeil Oliver, *The Neglected History of Criminal Procedure, 1850-1940*, 62 RUTGERS L. REV. 447, 505 n.319 (2010).

[57] Oliver, *supra* note 3, at 241-44.

[58] *Id.* at 244-45.

[59] *Acquit Kingsbury for Wiretapping: In Ordering Defendants Freed Court Says Evidence Did Not Indicate Bad Faith*, N.Y. TIMES, May 25, 1917, at 20.

[60] Oliver, *supra* note 3, at 245.

[61] *Id.*

Progressive Era, a period when the public was willing to place extraordinary trust in the police.

The famous, or infamous, Prohibition Era Supreme Court case *Olmstead v. United States* considered whether the Fourth Amendment placed limits on the power of the government to intercept telephone calls.[62] Not surprisingly, several telephone companies filed amicus briefs contending that intercepting a telephone call amounted to a search or seizure within the meaning of the Fourth Amendment. Much like telegraph companies before them, they had an interest in reassuring their customers that their privacy was being protected.

The efforts of these telephone companies were unsuccessful. A closely divided Court held that the Fourth Amendment does not protect the sounds that callers transmit from their homes.[63] The holding was destined to be short-lived. The trust the public was willing to place in the police during the Progressive Era would not survive Prohibition. Law enforcement during Prohibition proved itself to be incompetent at best and hopefully corrupt at worst. At the federal level, the United States Supreme Court quickly reversed the effect of the *Olmstead* decision, holding that the Communications Act of 1934 prohibited wiretapping, though the language the Court was interpreting could hardly be read to require—or even suggest—that conclusion.[64] In New York State, an unlikely interest group joined the fight against unregulated wiretapping—organized labor.

Organized labor's connections with organized crime made it a target for prosecutorial investigations, prompting labor's keen interest in civil liberties.[65] In the 1930s, organized crime began to infiltrate labor unions. Before Prohibition, gangs sold violence. The use of violence and its linkage to organized crime was certainly foreseeable, as alcohol became a legal product again. Arnold Rothstein, the infamous gangster alleged to have fixed the 1919 World Series, made a business of selling muscle to contending sides in labor strikes.[66] In the Garment Worker's Strike of 1926, he sold his product to both sides of the strike. Prohibition then created an easy and profitable market for contraband alcohol and made large criminal networks possible.[67]

---

[62] 277 U.S. 438 (1928).

[63] *Id.* at 463-65.

[64] Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of E-Mail,* 10 MICH. TELECOMM. & TECH. L. REV. 1, 28-31 (2003) (observing that the Supreme Court in the 1930s interpreted the Telecommunications Act of 1934 to forbid wiretapping and that Congress did not modify the statute to permit wiretapping until the late 1960s).

[65] *See* Oliver, *supra* note 56, at 521-22. William Nelson has described labor's support for limits on wiretapping and searches as part of a struggle between elites for order and non-elites for security from the elite's order-restoring apparatus. William E. Nelson, *The Changing Meaning of Equality in Twentieth Century Constitutional Law,* 52 WASH. & LEE L. REV. 3, 22 (1995). The linkage between organized labor and organized crime seems to provide a tighter explanation.

Prohibition both distracted organized crime from the violence racket and made criminal organizations much more sophisticated. The end of Prohibition took away the easiest source of their income but did not destroy the criminal organizations. Bootleggers became mobsters; former peddlers of contraband infiltrated legitimate businesses. For a variety of reasons, organized labor became an easy target for mob infiltration.

For legitimate and illegitimate reasons, labor was opposed to wiretapping. Trade unions were infiltrated by organized crime in the 1930s.[68] In New York, mob-busting prosecutor Thomas Dewey focused on these groups.[69] Corrupt unions obviously opposed his efforts to ferret out their wrongdoing. Legitimate unions objected to the unwelcomed government eavesdroppers itching to cobble together probable cause for an indictment.

Labor groups specifically asked the New York Constitutional Convention of 1938 to forbid wiretapping except when judicially authorized.[70] Their fear of government intrusion extended beyond eavesdropping. They asked the convention to include a provision that excluded illegally obtained evidence from criminal trials.[71] Labor interests were so powerful that not only did the New York

---

[66] DAVID PIETRUSZA, ROTHSTEIN: THE LIFE, TIMES AND MURDER OF THE CRIMINAL GENIUS WHO FIXED THE 1919 WORLD SERIES (2003); BENJAMIN STOLBERG, TAILOR'S PROGRESS: THE STORY OF A FAMOUS UNION AND THE MEN WHO MADE IT 138 (1944).

[67] STOLBERG, *supra* note 66, at 138.

[68] EDWARD BEHR, PROHIBITION: THIRTEEN YEARS THAT CHANGED AMERICA 238 (1996); SELWYN RAAB, FIVE FAMILIES: THE RISE, DECLINE, AND RESURGENCE OF AMERICA'S MOST POWERFUL MAFIA EMPIRES 37 (2005).

[69] MARY M. STOLBERG, FIGHTING ORGANIZED CRIME: POLITICS, JUSTICE AND THE LEGACY OF THOMAS E. DEWEY 50-51 (1995).

[70] 4 STATE OF NEW YORK, REVISED RECORD OF THE CONSTITUTIONAL CONVENTION OF THE STATE OF NEW YORK 3441 (1915).

[71] *Id.*

Constitution of 1938 require judicial authorization for a wiretap, but the proposed provision to make the exclusionary rule part of the Constitution barely failed in the convention.[72] The exclusionary rule has, of course, been one of the most popularly maligned rules of criminal procedure, comparable only with the public's distaste for the warnings arrestees must be given under *Miranda v. Arizona*.[73]

At the national level, a variety of labor groups similarly argued that Congress should forbid wiretapping. In 1941, a variety of labor groups—including the American Federation of Labor (AFL) and the Congress of Industrial Organizations (who were separate groups at this point)—joined a host of other labor organizations including the Brotherhood of Railway Trainmen, the American Newspaper Guild, the United Federal Workers of America, and the Steel Workers Organizing Committee in opposing wiretapping.[74] Like their labor counterparts who advocated limits on wiretapping in the New York Constitution a few years earlier, these labor organizations raised generic concerns about the power of the government to eavesdrop on its citizens.[75] The American Federation of Labor additionally observed that unions had a unique concern. The government, as the AFL observed, may assert an interest in strike busting in an actual, or claimed, interest in national security.[76] Highly influential labor groups thus joined the logical opponents of wiretapping—telephone companies—in opposing the power of government to intercept telephone calls.

V. THE NEXT COMMUNICATIONS REVOLUTION

As we enter our second communications revolution, no group has emerged with the influence of organized labor in the 1930s, or with the purity of interest of Western Union in the 1870s. As before, and predictably, a gap exists between the new technology and the law that will protect the privacy of customers using the new technology. However, it is not clear that the gap will be filled this time. Under the Electronic Communication Privacy Act of 1986, the government can obtain access to e-mails, mobile location information, information stored in computer "clouds," and information in social networking sites by demonstrating that the information is merely "relevant" to a criminal investigation.[77]

---

[72] WILLIAM E. NELSON, THE LEGALIST REFORMATION: LAW, POLITICS AND IDEOLOGY IN NEW YORK, 1920-80, at 125-27 (2001).

[73] 384 U.S. 436 (1966).

[74] *To Authorize Wiretappings: Hearing on H.R. 2266 and H.R. 3099 Before the H. Comm. on the Judiciary*, 77th Cong. 34, 75, 100, 131, 171, 237 (1941).

[75] *Id.* at 34-35, 76-77, 91-94, 131-32.

[76] *Id.* at 35.

As the social world moves from telephones to cell phones, e-mails, texts, and instant messages, it is hardly satisfactory to say that the degree of privacy varies with the manner of technology chosen. As the world evolves to cell phones, the land-line holdout cannot expect to be a part of a business and social world that now expects everyone to carry telephone and e-mail service in a pocket or purse.[78] As text messaging replaces cell phone calls, the person who cannot or will not use text messaging is left out. To do business, or be social, we must use technology not yet protected from the government's prying eye. Insisting on a manner of communication with greater legal protections for ordinary conversation is reminiscent of the television sitcom spy Maxwell Smart's constant insistence on using the awkward and inconvenient cone of silence to prevent interception.[79]

The use of new technology is thus, on some level, essential. Legislative innovations to protect privacy in these technologies is, however, certainly not inevitable. The degree of privacy we enjoyed from government interception of telegraphed messages (enjoyed before Western Union sent its last telegraph, that is), and enjoy from government intrusion on telephone calls, did not accompany these new technologies from their inception. The new forms of communication were not initially covered by laws limiting older forms of communication. Despite Western Union's arguments, telegraphs were not regarded to have inherited the legal protections afforded items sent through the mail. Despite statutory prohibitions on any interception of telephone calls, government snoops were believed to have limitless powers to tap telephones wires. Powerful advocacy groups convinced lawmakers to extend the privacy protection to new forms of communication. No similar groups appear on the horizon to ensure that privacy interests in these new modes of media technology will be protected.

---

[77] *See* 18 U.S.C. § 2511(2)(i)(III) (2006) ("It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if . . . (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation . . . .").

[78] Justice Kennedy recognized that:

> Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own.

City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010).

[79] *Biography for Don Adams*, IMDB, http://www.imdb.com/name/nm0010915/bio (last visited Jan. 22, 2012) (documenting that NBC hired Don Adams to star as Maxwell Smart, the "bumbling yet intrepid secret agent," in the Mel Brooks and Buck Henry spy spoof *Get Smart* in 1965).

No technology provider is poised to do the advocacy work of a nineteenth-century Western Union or an early-twentieth century Atlantic Telegraph and Telephone Company. Presently an organization called Digital Due Process is lobbying Congress to update the Electronic Communications Privacy Act (ECPA) to require greater protection from government intervention in new technologies.[80] The group includes unlikely partners like America Online, Apple, Americans for Tax Reform, the American Civil Liberties Union, and AT&T (to take a demonstrative sample whose sole common characteristic seems to be preserving alliteration in the list).[81]

There are reasons to believe this unlikely collection of actors will not be successful. Unlike Google or AOL, neither Western Union nor AT&T came to legislators or courts with unclean hands.

---

[80] *ECPA Reform: Why Now?*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=26802940-3840-11DF84C7000C296BA163 (last visited Jan.. 22, 2012) (discussing the latest news on ECPA reform and related issues); *see also* Gautham Nagesh, *Sen. Leahy Introduces Update to Digital Privacy law*, HILL (May 17, 2011, 1:54 PM), http://thehill.com/blogs/hillicon-valley/technology/161691-sen-leahy-introduces-update-to-digital-privacy-law.

[81] Other high profile members of this organization include eBay, Facebook, Google, IBM, and the Newspaper Association of America. *See Who We Are*, DIGITAL DUE PROCESS, http://www.digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163 (last visited Jan. 22, 2012).

Google, AOL, and others examine the content of e-mail messages to sell IP addresses to manufacturers interested in selling me quality barbeque sauce and single barrel bourbon, for instance.[82] Google, AOL, and others then are not the best champions of liberty when they ask Congress to place limits on the government's ability to acquire information about drug dealing or terrorist plots.

Similarly, there is no consumer group positioned to take over the role that organized labor played in the privacy debates. Unlike Western Union in the late 1800s or AT&T in the early 1900s, organized labor's hands were far from clean, though they may not have been as thoroughly dirty as Thomas Dewey suggested. Organized labor did, however, have influence in Congress and state legislatures that the ACLU could never boast.[83]

Finally, and perhaps most importantly, there seems to be less public concern over privacy at the turn of the twenty-first century than there was at the turn of the twentieth century. Corporations do not expect protecting privacy to be essential to retaining existing customers and attracting new ones. Qwest alone resisted the government's requests to tap the international calls of its subscribers as part of the National Security Agency's highly controversial wiretap program during the presidency of George W. Bush.[84]

With Facebook and Twitter, Americans themselves have grown accustomed, not necessarily to government eavesdropping, but to broadcasting virtually every detail of their lives to anyone who cares to surf the web. When a telegraph operator in the nineteenth century read a message he conveyed, it was not because the sender desired him to know the contents. When a telephone operator, or nosey member of a party line, listened in on a conversation in the early twentieth century, it was not because the parties to the conversation wished to broadcast their discussion. In modern society, discussions that are seemingly relevant to only two people appear on publically viewable Facebook walls or Twitter feeds. Companies like Facebook, AOL, and Google introduced us to the ability to broadcast every detail of our lives and feed our addiction to do so.

---

[82] *See, e.g.*, Schmidt, *supra* note 7.

[83] *See generally About the ACLU*, ACLU, http://www.aclu.org/about-aclu-0 (last visited Jan. 22, 2011) ("The ACLU also works to extend rights to segments of our population that have traditionally been denied their rights, including people of color; women; lesbians, gay men, bisexuals and transgender people; prisoners; and people with disabilities.").

[84] *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at A1.

We are no longer a private people. We live out loud. Perhaps quite naturally, there is no one poised to vigorously represent privacy concerns in these new technologies.

THE NEW REALITY OF SEARCH ANALYSIS: FOUR TRENDS CREATED BY NEW SURVEILLANCE TECHNOLOGIES

*Ric Simmons**

INTRODUCTION 991
I. THE RISE OF CONGRESS 995
II. FROM A BINARY ANALYSIS TO A SPECTRUM OF STANDARDS 999
III. INCREASED DEFERENCE 1005
IV. DOCTRINES OF CONFUSED FORMALISM 1009
CONCLUSION 1015

INTRODUCTION

The Fourth Amendment was drafted and ratified in a radically different world than that in which we live today. The political, social, and economic realities of the late eighteenth century created different concerns than those we face in the early twenty-first century. But, the most important changes we have seen over the past two hundred years—and the most important changes which will affect search analysis in the near future—are scientific in nature: new technologies which have revolutionized both how individuals commit crime and how law enforcement investigates it.

The primary way new technologies have altered the landscape of search analysis is by enabling law enforcement

---

[*] Professor of Law, Moritz College of Law, The Ohio State University. Funding for this work was underwritten by the National Center for Justice and the Rule of Law at the University of Mississippi School of Law, which is supported by a Grant awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position of the United States Department of Justice.

officials to conduct surveillance in new, often more intrusive, ways. As law enforcement officials employ these new technologies, courts must apply the Fourth Amendment to determine whether the new kind of surveillance constitutes a "search" at all and, if so, what showing the government must make in order to legally conduct the search. In cases involving electronic eavesdropping,[1] thermal imagers,[2] and hidden video cameras,[3] the courts have had to decide how the Fourth Amendment limits law enforcement's power in new ways that the Framers never imagined.

But, there is also another, more subtle way in which new technologies have influenced Fourth Amendment jurisprudence—they have enabled criminals to commit new types of crimes or commit traditional crimes in new ways that are much more difficult to detect and prevent. A child pornographer who wanted to distribute his goods was previously limited by very tangible, practical constraints regarding the number of pictures he could distribute and the number of people to whom he could distribute them; today, computers and e-mail make such limits obsolete. A teenage vandal in past eras might break store windows or spray-paint graffiti on walls; today, the same teenager might write a computer virus and cause millions of dollars worth of damage. An anarchist in the nineteenth century might seek to assassinate a president or plant dynamite in an opera house; his twenty-first century counterpart is able to destroy cities with nuclear weapons or poison an entire society with chemical or biological agents. Criminals now utilize encryption and cell phones to further their ends and hide deadly explosives in small backpacks or suitcases. Law enforcement, understandably, has engaged in aggressive counter-measures to prevent these crimes and apprehend the criminals who commit them. They have invaded suspects' computers to record their keystrokes,[4] they have read e-mails stored on remote servers,[5] and they have indiscriminately searched passengers on planes[6] and subway trains.[7]

---

[1] *See* Katz v. United States, 389 U.S. 347 (1967).

[2] *See* Kyllo v. United States, 533 U.S. 27 (2001).

[3] *See* United States v. Torres, 751 F.2d 875 (7th Cir. 1984).

[4] *See* United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

[5] *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

[6] *See* United States v. Edwards, 498 F.2d 496 (2d Cir. 1974).

[7] *See* MacWade v. Kelly, 460 F.3d 260 (2d Cir. 2006).

These twin effects of technology have dramatically impacted search analysis. This Article will examine four interconnected ways new technologies have affected how courts analyze government searches: the tendency of Congress to supplement the Fourth Amendment with legislation, the shift from a "binary" approach to a "spectrum" approach in categorizing surveillance methods, a heightened deference to the legislature and to the executive with regard to new surveillance technologies, and a troubling tendency of courts to misunderstand new surveillance technology and thereby create overly formalist tests. This last phenomenon occasionally leads Congress to step into the area to correct the mistake, thus beginning the cycle anew.

The first trend stems directly from the rapid pace of technological advancement and the mistakes courts make when they try to regulate these new technologies. These mistakes have encouraged Congress to step in and create its own rules regulating law enforcement's use of technology or curtailing the use of technology by criminals. Thus, most judges conducting a modern day search analysis must go beyond the text and jurisprudence of the Fourth Amendment and its associated jurisprudence; they must also interpret one (or more) of a dozen or so federal provisions limiting the use of technology by law enforcement, from the Federal Communications Act of 1934[8] through the USA PATRIOT Act of 2001.[9] And although these statutory provisions are theoretically secondary to the protections of the Fourth Amendment, they have also had a feedback effect on how courts interpret the Fourth Amendment.

The second trend has been a shift away from a "binary" approach, in which the court's only job was to decide whether a certain type of surveillance is or is not a search, to a "spectrum" approach, in which a court must determine the level of invasiveness of the search in order to choose the appropriate restrictions to impose on the search. This trend famously began in 1968 with *Terry v. Ohio*, when the Supreme Court held that a pat-down is not a "search" but nevertheless implicates the Fourth Amendment.[10] This created a new category of surveillance ("*Terry* stops") and a new standard for evaluating surveillance in this category (reasonable suspicion). Congressional interference in surveillance regulation has accelerated this trend substantially, adding more layers to the spectrum.

---

[8] *See* 47 U.S.C. § 605 (2006).

[9] *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[10] 392 U.S. 1, 30-31 (1968).

Congressional interference has also accelerated the third trend. Because so many statutes now regulate surveillance methods, courts are far more likely than they were in the past to defer to Congress in analyzing surveillance techniques. In fact, as we will see, courts have even adopted statutory standards and imported them into their Fourth Amendment jurisprudence, effectively allowing Congress to interpret the contours of the Fourth Amendment. But, courts are not only showing greater deference to the legislative branch; they have also become more deferential to law enforcement as well. Since new technology enables criminals to hide their activities more effectively—and cause more damage when they succeed in those activities—courts are more likely to defer to law enforcement officers when they employ more aggressive tactics to detect these criminals.

Finally, new surveillance technology has occasionally created confusion among judges, thus further complicating the jurisprudence of search analysis. In such cases, courts have resorted to overly formalist doctrines that fail to reflect the reality of how the technologies actually work. Frequently, these doctrines persist for decades before the courts correct them—as was the case in *Olmstead v. United States*,[11] which created a "property-based" concept of search analysis that persevered for forty years before it was overruled by *Katz v. United States*.[12] The most blatant existing example of this formalism—the third-party consent doctrine of *Smith v. Maryland*[13]—is only now being challenged by courts, over thirty years after its birth.

Luckily, the damage done by such formalist doctrines has been limited because the courts' most blatant mistakes have been corrected by Congress. In this sense, congressional interference may be seen as a positive development, or at the very least, as inevitable. The following Section examines the ways in which

---

[11] 277 U.S. 438, 466 (1928).

[12] 389 U.S. 347, 353 (1967).

[13] 442 U.S. 735 (1979); *see infra* notes 74-78 and accompanying text.

Congress has delved into the regulation of surveillance technology.

I. THE RISE OF CONGRESS

Historically, the Fourth Amendment, as interpreted by the courts, has acted as the primary restriction on the government's authority to search its citizens. A generation ago, scholars studying search and seizure could safely ignore statutes, and judges rarely went beyond Fourth Amendment jurisprudence in deciding search and seizure cases. Today, however, anyone who wants to understand search analysis in the context of new surveillance technologies must be familiar with the numerous statutes now dominating the field.

The first major foray by Congress into regulating government surveillance came in 1934. Predictably, the legislation came in response to a new technology the Supreme Court failed to understand and, thus, failed to regulate properly—the telephone. In the 1928 case of *Olmstead v. United States*, the Supreme Court held that the government did not conduct a "search" under the Fourth Amendment when it wiretapped a telephone.[14] The Court's reasoning betrayed its lack of understanding of how this new communications technology interacted with basic privacy rights. As a result of this misunderstanding, the Court resorted to a simplistic formalism to reach a disastrous conclusion: "The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment."[15]

This infamous "property-based" test for determining whether a search occurred remained in use until overturned by *Katz* forty years later.[16] In Part IV, we will see how new surveillance technologies frequently lead to this kind of formalism,[17] which may take decades to correct. With regard to the specific case of telephone wiretapping, Congress decided it could not wait for the courts to fix the mistake, and so the legislature stepped in to protect an individual's privacy interests by passing the Federal Communications Act of 1934, which prohibited intercepting and disclosing any information that passes over telephone lines.[18]

---

[14] 277 U.S. 438, 466 (1928).

[15] *Id.*

[16] *Katz*, 389 U.S. at 353.

[17] *See infra* note 71 and accompanying text.

Since 1934, congressional intervention into surveillance regulation has grown exponentially, accelerating in recent decades. Among the more prominent examples are: Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III),[19] which regulates oral and wire communications; the 1986 Electronic Communications Privacy Act (ECPA),[20] which extends Title III to electronic communications; the Stored Communications Act (SCA),[21] which was part of ECPA and regulates government access to stored wire and electronic communications held by third-party internet service providers (ISPs); the Foreign Intelligence Surveillance Act of 1978 (FISA),[22] which sets out rules for electronic surveillance of agents of foreign powers; and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act),[23] which, among other effects, broadens the type of surveillance allowed under FISA and the ECPA.

In some ways, the relationship between the courts and the legislature in this context is typical: the legislature creates a statute, and the courts evaluate it in light of the Fourth Amendment and occasionally strike down the statute as unconstitutional. This was the process that occurred in the late 1960s—New York State passed a law regulating wiretapping,[24] and the Supreme Court, in *Berger v. New York*,[25] overturned the law as inconsistent with the Fourth Amendment.[26] Congress responded in 1968 with Title III, which provides stronger protections than the New York statute had created. Similarly, the PATRIOT Act of 2001 amended FISA to allow "sneak and peek" warrants—search warrants, which could be exercised before notification was given to the suspect—if a "significant purpose" (rather than a "primary purpose") of the search was gathering foreign intelligence.[27] In 2007, a federal judge struck down this provision as inconsistent with the Fourth Amendment,[28] though her decision was later overturned on procedural grounds.[29]

---

[18] *See* 47 U.S.C. § 605 (2006).

[19] *See* 18 U.S.C. §§ 2516-2518 (2006).

[20] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[21] *See* Stored Wire and Electronic Communications and Transactional Records Access, ch. 121, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2701-2712 (2006)).

[22] *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978).

[23] USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[24] N.Y. CRIM. PROC. § 813-a (McKinney 1958), *overturned by* Berger v. New York, 388 U.S. 41 (1967).

[25] 388 U.S. 41 (1967).

But, this traditional relationship between courts and the legislature is not the whole story. In the context of regulating new surveillance technologies, the relationship between the courts and the legislature is a bit more complicated. Legislatures frequently create protections above and beyond what the Fourth Amendment requires—which leads to problems when citizens rely on these protections as though they are constitutionally protected, only to find them repealed by later statutes.

An example of this phenomenon can be found in the laws regulating wiretapping. Under Title III, law enforcement is required to show more than mere "probable cause" before conducting this type of surveillance. Instead, it must meet a much higher standard, including demonstrating that normal investigative procedures are inadequate[30] and that the surveillance will be conducted in a way that minimizes the interception of irrelevant communication.[31] These Title III requirements have never been reviewed by the Supreme Court, but they have been unanimously approved by the appellate courts as *sufficient* to satisfy the Fourth Amendment.[32] Thus, it remains unknown whether they are *required* in order to satisfy the Fourth Amendment. As a result, when political tides shifted in the wake of the September 11th attacks, Congress felt free to relax some of the requirements of Title III.[33] Many were outraged by these changes,[34] partly because of the presumption that protections against unreasonable searches and seizures are based on the Constitution and, thus, insulated from the political whims of Congress. But, as Congress intervenes more and more often to regulate surveillance, we need to adjust to a new paradigm—one in which the balance that is struck between the needs of law enforcement and the privacy rights of individuals is constantly updated according to the prevailing political mood.

---

[26] *Id.* at 43, 64.

[27] 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B) (Supp. 2011).

[28] Mayfield v. United States, 504 F. Supp. 2d 1023, 1032, 1042-43 (D. Or. 2007), *vacated on other grounds by* Mayfield v. United States, 599 F.3d 964, 973 (9th Cir. 2010).

[29] *Mayfield*, 599 F.3d at 973.

[30] 18 U.S.C. § 2518(3)(c) (2006).

[31] 18 U.S.C. § 2518(5) (2006). Title III also limits the use of wiretapping to investigations of certain enumerated crimes, requires authorization by a high-level Justice Department official, and limits the duration of the order to thirty days (with the possibility of an extension). 18 U.S.C. §§ 2518(3)(a), 2516(1), 2518(5) (2006).

In theory, the Fourth Amendment still provides a baseline minimum of privacy, protected by the courts. In practice, however, a more subtle shift is occurring—as Congress becomes more and more involved in this field, the Supreme Court is showing more and more deference to congressional rules about the appropriate level of regulation. This increased deference is discussed in Part III of this Article.[35]

Scholars are currently engaged in a debate as to whether the increase in congressional involvement is a positive or a negative trend. Proponents of judicial supremacy in this realm, such as Lawrence Lessig, have argued that courts must apply consistent constitutional values to all types of surveillance, whether or not the surveillance involves new technologies.[36] Professor Orin Kerr has taken the opposite view, arguing that the legislature is better equipped to determine the proper balance between the needs of law enforcement and the privacy rights of individuals.[37] But regardless of whether this is a desirable trend, it seems certain to continue or even accelerate in the future; meaning that scholars, judges, and law enforcement officers must be well-versed in both Fourth Amendment jurisprudence and the myriad of congressional provisions that regulate high-tech surveillance.

---

[32] *See, e.g.*, United States v. Tortorello, 480 F.2d 764, 774-75 (2d Cir. 1973); United States v. Cafero, 473 F.2d 489, 501 (3d Cir. 1973); United States v. Cox, 462 F.2d 1293, 1304 (8th Cir. 1972); United States v. Cox, 449 F.2d 679, 687 (10th Cir. 1971).

[33] The PATRIOT Act, for example, allowed wiretapping under much lower FISA standards as long as the "significant" purpose of the surveillance was counterintelligence, rather than the "sole" purpose. *See* USA PATRIOT Act, tit. 2, § 218, 115 Stat. 272, 291 (2001). The Protect America Act of 2007 allowed warrantless wiretapping of United States citizens if the call began or ended in a foreign country. *See* Pub. L. No. 110-55, § 2, 121 Stat. 552, 553-55 (2007) (codified as amended at 50 U.S.C. § 1805 (2006)).

[34] *See, e.g.*, *ACLU Response to the Protect America Act of 2007*, ACLU (Aug. 7, 2007), http://www.aclu.org/national-security/aclu-fact-sheet-%E2%80%9Cpolice-america-act.

[35] *See infra* notes 56-64 and accompanying text.

[36] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 216 (1999).

II. FROM A BINARY ANALYSIS TO A SPECTRUM OF STANDARDS

The increase in congressional involvement in regulating surveillance of new technologies has accelerated another important trend in this field: the shift from a binary analysis, in which courts would simply decide whether or not a "search" has occurred, to an ever-expanding spectrum of choices, in which courts (or legislatures) must determine the level of invasiveness of the surveillance and then determine what requirements law enforcement must meet in order to conduct the surveillance. Only a few decades ago, there was only one question courts had to answer: did the surveillance implicate the Fourth Amendment? If so, a warrant (supported by probable cause) was required. If not, the surveillance was completely unregulated by law.

Perhaps the most famous recent Fourth Amendment case concerning new technologies involved such a binary analysis. In *Kyllo v. United States*,[38] the Supreme Court decided whether law enforcement officers conducted a "search" when they used a thermal imager to detect telltale signs of heat lamps used to grow marijuana inside a house.[39] But *Kyllo*, and the analysis that the Court conducted to decide the case, are now the exception in surveillance regulation. In most modern cases, especially those involving new technologies, courts may decide that the surveillance implicates the Fourth Amendment but not to the degree that probable cause is required—or perhaps to such a great degree that something *more* than probable cause is required. And, as we have seen in the previous Section, the surveillance may not implicate the Fourth Amendment, but it may be regulated by any number of statutes, which set out a variety of different standards for law enforcement to satisfy.

---

[37] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 864-82 (2004). Kerr notes that technological change advances quite rapidly, and legislatures, not courts, are in the best position to respond to this rapid change, since they (1) can make policy decisions before cases and controversies arise, rather than being reactive; (2) can change statutory regulation much more quickly than courts can change doctrine; and (3) have access to broad inputs of information not available to courts. *Id.*

[38] 533 U.S. 27 (2001).

[39] *Id.* at 29-30.

To be sure, neither Congress nor new surveillance technologies began this trend. The first real break from the binary analysis was in *Terry v. Ohio*,[40] in which the Supreme Court famously held that "a rigid all-or-nothing model of justification and regulation under the [Fourth] Amendment" was inadequate.[41] Instead, the Court took a broader view of "reasonableness" and applied the concept not merely to determine whether a search occurred, but also to conduct a balancing test between the intrusiveness of the search and the needs of law enforcement.[42] The result was a new standard: reasonable suspicion that "criminal activity may be afoot and that the persons with whom he is dealing may be armed and presently dangerous."[43] Other deviations from the binary analysis can also be found outside the context of new technologies, such as no-knock search warrants[44] and bodily intrusions,[45] both of which require a stronger showing than mere probable cause.

But, it is the context of new technologies—both those used by suspects and those used by investigators—which has provided the most frequent source of new standards for surveillance analysis. We have already seen that wiretapping and video surveillance are only permissible if law enforcement can satisfy the rigorous requirements of Title III—either because Title III directly applies (as in wiretapping) or because the courts have imported the high standards of Title III into constitutional law (as in video surveillance). Taken with the *Terry* doctrine, the Title III requirements result in four different "levels" of surveillance: those which are unregulated by the Fourth Amendment (such as surveillance from an aircraft[46]); those which require reasonable suspicion (such as a *Terry* stop); those which require probable cause and a warrant (such as a standard search of a home); and those which must meet the Title III requirements (such as covert video surveillance).

---

[40] 392 U.S. 1 (1968).

[41] *Id.* at 17.

[42] *Id.* at 19-20.

[43] *Id.* at 30.

[44] Wilson v. Arkansas, 514 U.S. 927, 934 (1995).

[45] Winston v. Lee, 470 U.S. 753, 759 (1985).

As noted in the above section, Congress has stepped in to add many more "levels" of searches. When law enforcement is seeking "address" information, such as the phone numbers dialed by a suspect or the "from" line of an e-mail, the investigator must only demonstrate "certified relevance,"[47] and the judicial role in reviewing this standard is "ministerial in nature."[48] If law enforcement is seeking "historic information" (such as subscriber records in an online database, or a stored e-mail which has already been opened by the recipient), the investigator must show "specific and articulable facts."[49] However, if the e-mail has not yet been opened, a warrant is required,[50] and if the e-mail is captured "in transit" as it is being sent, then it is considered "electronic communication" and a Title III warrant is required.[51] To further complicate the matter, new congressional acts can change the standards required for any particular kind of search, as we saw in the previous Section when the PATRIOT Act modified the rule for wiretapping telephone calls if a "significant purpose" of the surveillance was counter-intelligence.[52]

This shift raises two interesting questions. The first question is whether this "sliding scale" of surveillance regulation is an improvement on either the binary analysis of the past or the tertiary analysis that existed post-*Terry*. Certainly the new regime may be problematic for law enforcement officers who have to decode and memorize an ever-increasing number of standards and digest even more case law surrounding the standards. Fourth Amendment jurisprudence was already challenging enough when police officers on the street seeking to search a car or an individual had to comply with shifting standards of "reasonableness" to determine whether their actions were legal. Now, law enforcement officers who conduct electronic surveillance must learn even more law in order to ensure they are in compliance. Granted, the nature of electronic surveillance means that these decisions do not have to be made in the split-second pressures of most street encounters, but we ought to be aware that by shifting to a spectrum analysis, we are asking for a significant amount of legal expertise on the part of law enforcement officials. In other words, a tension exists between drafting the most precise rule for each situation and creating rules that are simple enough for law enforcement to apply properly and consistently.

---

[46] *See* California v. Ciraolo, 476 U.S. 207 (1986).

[47] 18 U.S.C. § 3122(b)(2) (2006). This was a provision of the 1986 ECPA.

[48] United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995).

[49] 18 U.S.C. §§ 2701-2712 (2006). These were provisions of the Stored Communication Act ("SCA"), another aspect of the 1986 ECPA.

[50] *Id.*

[51] 18 U.S.C. § 2518 (2006).

[52] *See* USA PATRIOT Act of 2001, tit. 2, § 218, 115 Stat. 272, 291 (2001).

Another concern is the effect the sliding scale has on privacy rights. Some would argue that a spectrum of different standards actually increases privacy rights because courts (and legislatures) that would be reluctant to require a full-blown warrant might be willing to regulate lower-level forms of surveillance with weaker standards. For example, Congress may not think it wise to require a law enforcement officer to obtain a warrant before she can subpoena the telephone numbers for all incoming and outgoing calls on a specific line; so if there were no lower standard available, the law enforcement officer would be able to acquire this information with no regulation whatsoever. And on the other end of the spectrum, privacy rights are certainly enhanced by requiring more intrusive searches to be regulated more tightly than a standard search of a residence.

Once the standards of probable cause and warrant get watered down, however, there is the danger of a slippery slope—more and more types of searches may be "downgraded" to an easier standard—especially as Congress begins to assert more dominance in this field. And the requirements on the lower end of this spectrum are not very impressive—a requirement of "certified relevance" or "specific and articulable facts" will not do much to protect an individual's privacy rights if law enforcement is determined to obtain the information.

The second question surrounding the shift to a spectrum analysis concerns the logical consistency of the different standards on the sliding scale. As Professor Christopher Slobogin pointed out in a recent book, the Supreme Court has not created a consistent framework for this new spectrum of standards, nor has it explained the direct relationship between the intrusiveness of the surveillance and the standard the government must meet to conduct the surveillance.[53] And certainly, Congress has not made an effort to create such a framework; it adds on new standards for different types of searches without any need to explain how the many different standards fit together.

Professor Slobogin proposes a "proportionality principle" to deal with this question in which courts (and presumably legislatures) would assess the invasiveness of the surveillance and the needs of law enforcement before setting standards accordingly.[54] The problem with this approach is how to determine the level of "invasiveness" of each type of surveillance.[55] Are we meant to look to society's perceptions of privacy? If so, does that mean the sliding scale would need to be adjusted as perceptions of privacy change? In today's world, notions of privacy are changing rapidly as information becomes more and more accessible. Individuals put an unprecedented amount of private information into the public arena—both intentionally and unintentionally. Many individuals choose to use new technologies to make their private lives more public. Diaries, which were once kept hidden under mattresses, are now posted on blogs, along with personal pictures and messages from friends. Telephone conversations that used to occur in homes or private phone booths are now carried out on the street and in malls, stores, and other public areas.

On the other side of the balance of proportionality, how do we evaluate the needs of law enforcement? In many ways, technology has actually *increased* our ability to keep things secret from the government. Take two simple examples: data storage and communications. Only 150 years ago, a diary writer or record keeper had very limited options as to how to secretly record and store his writings. In modern times, the diary or records could be written on a laptop computer, accessible only by someone with the password or stored on a hard drive the size of a pen and hidden almost anywhere. The same analysis holds true for the confidentiality of communication. Two hundred years ago, a person who wished to communicate with someone else had to either travel to their house in person or send a letter with the address of the letter visible for all to see and the contents accessible by merely ripping open the envelope. Modern communications involve cell phones, e-mails, and encrypted information—all of which require sophisticated technical equipment to intercept and decode. Meanwhile, the Internet allows individuals to stay in the privacy of their own homes to conduct many activities which formerly had to be done in public: shopping, searching for information, downloading pictures and movies, and so on. Only twenty years ago, almost any of these tasks required the average person to leave her home and publically visit any number of businesses, which would have subjected the person to easy (and unregulated) surveillance by law enforcement.

---

[53] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 38 (2007).

[54] *Id.* at 31. Slobogin proposes five different levels of standards: (1) no regulation at all, (2) "relevance" (which translates roughly to a 5% chance criminal activity will be detected), (3) "reasonable suspicion (30% chance), (4) probably cause (50%), and (5) clear and convincing (75%). *Id.* at 38-41.

[55] To be fair, this is a problem inherent in any attempt to impose an overarching framework on the spectrum of surveillance types. Slobogin himself acknowledges some critics say his proposal "would convert the Fourth Amendment 'into one immense Rorschach blot.'" *Id.* at 46 (quoting Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 393 (1974)). Amsterdam also called the proportionality principle "splendid in its flexibility [but] awful in its unintelligibility, unadministrability, unenforcibility and general ooziness." Amsterdam, *supra*, at 415.

Thus, what at first seem to be insidious new methods of eavesdropping and snooping—wiretapping phones, monitoring e-mails, searching computer hard drives—are simply remedial measures on the part of the government in an attempt to maintain the appropriate balance between individual privacy and effective law enforcement. In other words, privacy-enhancing technology has arguably increased (and will continue to increase) the justification for law enforcement surveillance.

These concerns are still problematic in a one-size-fits-all binary analysis, but to a much smaller degree. Most types of surveillance are either clearly "searches" requiring warrants or are not, and, therefore, not subject to regulation. Under such a simplified regime, evolutions of technology only rarely—as in the *Kyllo* case—bring new challenges. In short, the new (and expanding) spectrum of surveillance standards brings us better precision, but it is vulnerable to confusing ambiguity, especially as societal perceptions of privacy change and privacy-enhancing technology increases the justification for invasive surveillance.

III. Increased Deference

A third trend in the regulation of new surveillance technology—one which also has been accelerated by the increased activity of Congress in this area—is the greater level of deference courts give to Congress and to law enforcement. We have already seen Congress enact numerous statutes to regulate new surveillance technologies, in some cases replacing the Fourth Amendment as the primary source of protection against invasive searches. This increased involvement leads courts to defer to Congress in two ways: first, courts are increasingly likely to stand back and wait for Congress to act when new surveillance technologies arise; and second, when courts do act, they occasionally borrow Congress's own regulatory scheme in interpreting the Fourth Amendment.

An example of the first type of deference to Congress can be found in the regulation of wiretapping, an area where Congress has been especially active. As the Fourth Amendment scholar Orin Kerr has argued, "the existence of the statutory Wiretap Act effectively displaces any constitutional remedies that in theory should exist under cases like *Katz* and *Berger*."[56] Kerr gives the example of the wiretapping of cordless phone calls. Congress originally did not extend Title III protection to these calls, creating a significant gap in the law, since "conversations on land-line phones were protected by the Wiretap Act while conversations on cordless phones were not."[57] An active judiciary that was aggressively enforcing a minimum level of privacy rights that was guaranteed by the Fourth Amendment would have closed this gap, but the courts refused to do so.[58] Instead, the Fourth Circuit warned against "wield[ing] the amorphous 'reasonable expectation of privacy' standard in a manner that nullifies the balance . . . struck by Congress in Title III"[59] and affirmed that "the primary job of evaluating [new technologies'] impact on privacy rights and of updating the law must remain with . . . the legislature."[60] This and other examples led Kerr to conclude that "wiretapping law may be constitutional in theory, but it is statutory in practice."[61]

---

[56] Kerr, *supra* note 37, at 853.

[57] *Id.* at 852.

[58] *Id.*

[59] United States v. McNulty (*In re* Askin), 47 F.3d 100, 105-06 (4th Cir. 1995) (citation omitted).

A more dramatic instance of courts' deference to Congress occurred when courts sought to define the scope of constitutional parameters for covert video surveillance. As in the case of cordless phones, Congress failed to act in this area, since Title III explicitly excludes video surveillance from its purview.[62] But this time, instead of waiting for Congress to act, the courts showed even greater deference to Congress by holding that the Fourth Amendment protections for video surveillance were *identical* to the statutory requirements already set out by Congress for wiretapping. In *United States v. Torres*, the Seventh Circuit explained that it was "borrow[ing] the warrant procedure of Title III, a careful legislative attempt to solve a very similar problem, and hold[ing] that it provides the measure of the government's constitutional obligation of particular description in using television surveillance to investigate crime."[63] Since *Torres*, six other federal circuits have used the Title III safeguards to define the scope of the Fourth Amendment warrant requirement in the context of video surveillance.[64]

In short, when facing a clear gap in the surveillance regulations created by statute, the courts have responded in one of two ways: either by doing nothing, assuming that the Fourth Amendment does not apply in the context at all; or, if the gap is so blatant, that the Fourth Amendment *must* apply by simply borrowing the standards crafted by Congress in a different context and elevating them to the constitutional level.

---

[60] *Id.* at 106. Congress did indeed pass legislation extending Title III protection to cordless phones in 1994. *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 202, 108 Stat. 4279, 4290-91 (1994).

[61] Kerr, *supra* note 37, at 855.

[62] *See* United States v. Torres, 751 F.2d 875, 886 (7th Cir. 1984).

[63] *Id.* at 885.

[64] *See* United States v. Williams, 124 F.3d 411, 416 (3d Cir. 1997); United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992), *cert. denied*, 506 U.S. 1005 (1992); United States v. Mesa-Rincon, 911 F.2d 1433, 1437 (10th Cir. 1990); United States v. Cuevas-Sanchez, 821 F.2d 248, 252 (5th Cir. 1987); United States v. Biasucci, 786 F.2d 504, 510 (2d Cir. 1986), *cert. denied*, 479 U.S. 827 (1986).

Courts have also shown signs of deferring to law enforcement when considering the constitutionality of a new type of surveillance, especially if the government claims to be "responding" to new technologies being used by criminals. As noted above, new technology not only allows law enforcement to conduct more intrusive levels of surveillance, but it also allows criminals to hide their activities more effectively from law enforcement and to cause more damage as a result of their criminal activity. In these cases—when the government is reacting to new crimes or techniques employed by criminals—some courts have interpreted the Fourth Amendment narrowly, deferring to law enforcement regarding what is necessary to maintain public safety or counter a particular form of criminal activity.

Part of this deference stems from a legitimate desire to allow law enforcement to keep pace with criminals in the technological arms race that occurs between police and criminals. For example, criminals are increasingly using advanced cryptography on their communications and data storage. In order to combat this encryption in one case, FBI agents acquired a warrant and installed software on a suspect's computer that recorded the keystrokes as they were being typed, thus intercepting the suspect's password as he typed it.[65] The defendant moved to suppress the evidence that was found on the grounds that the FBI was actually intercepting a "wire communication" in transit, and therefore, a Title III order—not a mere warrant—was required.[66] The court rejected the defendant's argument and then gave this rather extraordinary explanation:

> In this day and age, it appears that on a daily basis we are overwhelmed with new and exciting, technologically-advanced gadgetry. Indeed, the amazing capabilities bestowed upon us by science are at times mind-boggling. As a result, we must be ever vigilant against the evisceration of Constitutional rights at the hands of modern technology. Yet, at the same time, it is likewise true that modern-day criminals have also embraced technological advances and used them to further their

---

[65] United States v. Scarfo, 180 F. Supp. 2d 572, 574 (D.N.J. 2001).

[66] *Id.* at 581-82.

> felonious purposes. Each day, advanced computer technologies and the increased accessibility to the Internet means criminal behavior is becoming more sophisticated and complex. This includes the ability to find new ways to commit old crimes, as well as new crimes beyond the comprehension of courts. As a result of this surge in so-called "cyber crime," law enforcement's ability to vigorously pursue such rogues cannot be hindered where all Constitutional limitations are scrupulously observed.[67]

Unfortunately, this doctrine of deferring to law enforcement officers when they are pursuing criminals who are "find[ing] new ways to commit old crimes" is ultimately unworkable. The problem is that there is no meaningful way to define when a criminal is using a "new" technology to commit or conceal his crime. As noted earlier, telephone communications could be considered a "new way" to commit a crime—and perhaps that was one of the unspoken reasons why the *Olmstead* Court deferred to law enforcement's warrantless tapping of the phones in 1928. But, it would not make sense to give law enforcement extra deference regarding telephone wiretapping merely because they are countering a new technology being used by criminals. Rather, the opposite is true: because of the intrusive nature of the surveillance, telephone wiretapping undoubtedly deserves the higher standard Title III has created for it. Likewise, *Kyllo* could be considered a "responsive" use of technology by law enforcement, since the defendant was using heat lamps to grow marijuana indoors rather than the traditional method of growing it out in the open, where it could be more easily seen.[68] But the Supreme Court correctly did not give law enforcement officers any special deference when the officers responded to the heat lamps with their own type of new technology to try to see through the walls of the house.

In short, courts have slowly abdicated their authority with regard to regulating new surveillance technologies. Some aspects of this deference, such as waiting for Congress to fill an obvious gap in existing legislation, may make sense. Other aspects, such as courts giving law enforcement officers greater leeway if they are "responding" to new technologies, may be more problematic.

---

[67] *Id.* at 583 (citation omitted).

[68] *See Kyllo v. United* States, 533 U.S. 27, 29-30 (2001).

IV. DOCTRINES OF CONFUSED FORMALISM

One final trend we can see in the regulation of new surveillance technology is courts occasionally demonstrate a lack of understanding about how these technologies actually work. These misunderstandings can lead to nonsensical, formalist legal doctrines, which may take decades to correct.

We have already seen one example of this in *Olmstead*; the Supreme Court held that because the defendant was "project[ing] his voice to those quite outside" the house, he had no privacy rights in the communication.[69] In other words, the Court saw the telephone more like a radio transmitter, sending information out into the world for public consumption. This may have been a misunderstanding of the technology of the telephone, or perhaps a misunderstanding of how telephone communications were perceived by society. But either way, it was a serious—and fateful—misunderstanding. The *Olmstead* decision created a formalist, "property-centered" doctrine of Fourth Amendment rights—one which would last for forty years—in which the Court would determine whether there was a violation of a defendant's Fourth Amendment rights merely by looking to whether a defendant's property rights had been infringed upon.[70]

Olmstead's mistake was eventually corrected,[71] but a danger still exists of formalist doctrines arising as a result of a court's misunderstanding the nature of new technology. The most infamous of these doctrines can be found in the case of *Smith v. Maryland*.[72] In *Smith*, police officers—acting without a warrant or court order—instructed the telephone company to record all of the telephone numbers the defendant dialed from his telephone line.[73]

---

[69] Olmstead v. United States, 277 U.S. 438, 466 (1928); *see also supra* notes 14-15 and accompanying text.

[70] *See, e.g.*, Silverman v. United States, 365 U.S. 505, 511-12 (1961); Goldman v. United States, 316 U.S. 129, 135 (1942).

[71] Its specific holding was reversed by the Federal Communications Act of 1934, 47 U.S.C. § 605 (2006); its doctrine was reversed by the "reasonable expectations of privacy" test of *Katz v. United States*, 389 U.S. 347, 353, 360 (1967).

[72] 442 U.S. 735 (1979).

[73] *Id.* at 737.

The Supreme Court held no warrant was necessary since the defendant had "voluntarily conveyed to [the phone company] information that it had facilities for recording and that it was free to record."[74] In this case, the Court's *holding* was probably correct—an individual has no reasonable expectation of privacy in the phone numbers he or she dials, any more than the individual has a reasonable expectation of privacy in the address on a letter (or the address on an e-mail). In fact, such "addressing" information is now explicitly covered by statute and is given one of the lowest levels of protection, requiring only a showing of "certified relevance."[75] But, the Court's *reasoning* in the *Smith* case was calamitous—just as calamitous (and for the same reason) as its reasoning in *Olmstead* over fifty years before. Under the *Smith* doctrine, an individual loses all privacy rights to any information that he or she voluntarily conveys to a third party. Even in 1979, this was a dubious rationale since many people stored confidential information (such as bank records)[76] with third parties or passed such information on to others using third parties (such as telephone companies or private messenger services). In modern times, when many people use cloud computing for storing data and third-party ISPs for transmitting, this rationale is patently absurd.

Luckily, some modern courts have recognized this absurdity and found ways to reject the *Smith* doctrine. In the recent case of *United States v. Warshak*,[77] the Sixth Circuit held that a third party's access to stored e-mail does not eliminate the warrant requirement.[78] The *Warshak* court first looked to "the prominent role that e-mail has assumed in modern communication,"[79] stating:

> People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with

---

[74] *Id.* at 745.

[75] *See* 18 U.S.C. § 3122(b)(2) (2006); *see also supra* note 47 and accompanying text.

[76] *See* United States v. Miller, 425 U.S. 435, 442 (1976).

[77] 631 F.3d 266 (6th Cir. 2010).

[78] *Id.* at 286-88.

[79] *Id.* at 284.

> the click of a mouse button. . . . In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities.[80]

After analyzing the generally accepted uses and expectations for e-mail, the *Warshak* court analogized e-mail to the content of telephone calls or traditional letters[81] and concluded "the ISP is the functional equivalent of a post office or a telephone company."[82] The court also analogized the relationship between an ISP and its stored e-mails to the relationship between a hotel and the rooms it rents to its guests, thus establishing that neither the ability nor the right to access the stored information by a third party nullifies the owner's reasonable expectation of privacy.[83] Finally, the court rejected applying the precedent of *United States v. Miller*,[84] a pre-cursor of *Smith* in which a bank depositor was held to have no privacy rights in the information he conveyed to his bank.[85] According to the *Warshak* court, *Miller* was distinguishable because the bank was the ultimate end recipient of the information, while the ISP in *Warshak* was an intermediary.[86]

In short, the *Warshak* court made the effort to truly understand how stored e-mails are used and perceived by modern society, instead of merely relying on the formalist third-party doctrine that was crafted in a different context (storage of bank records) and then clumsily pasted onto a new technology (as in *Smith*).

Other courts have also rejected the easy formalism that has plagued this area of the law. A district court in New York recently had to determine how much protection to give "pass-through" digits in a telephone call. Pass-through digits are the numbers dialed on a telephone after a connection is made—for example, digits that navigate through a phone tree or digits that communicate the caller's social security number or account number.[87] Although the government argued that these numbers should only receive the low-level protection afforded to dialed telephone numbers under the Pen/Trap statute,[88] the court looked to the *content* of the information being provided, which included "sensitive and personal" information such as "[b]ank account numbers, pin numbers and passwords, prescription identification numbers, social security numbers, credit card numbers, and so on . . . ."—the "functional equivalent" of what callers used to tell human operators.[89] When this information was considered in the proper context, the court had no problem confirming individuals had a reasonable expectation of privacy in the pass-through digits.[90]

---

[80] *Id.*

[81] *Warshak*, 631 F.3d at 285-86.

[82] *Id.* at 286.

[83] *Id.* at 287 (citing United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997)).

[84] 425 U.S. 435 (1976).

[85] *Id.* at 442-43.

[86] *Warshak*, 631 F.3d at 288.

Another recent case from the District of Massachusetts[91] also engaged in an admirably sensible—even prescient—analysis of a new technology. In this case, the question was the privacy afforded "historical cell site information"—that is, information subpoenaed from the cell phone company about the location of a cell phone at a time when a call is placed. The government argued these records were governed by the low standards of the SCA, requiring only a showing of "specific and articulable facts"[92] since it was only seeking stored "historical information" about the location of a caller at some time in the past when a call was placed.[93] The court, however, looked not to how the information was classified, but to how it would actually be used by the government as a tracking system, saying:

> In reality, the Government is seeking the issuance of an order that would technically permit the Government access to cell site information as early as one second prior to the

---

[87] *See In re* Applications for Pen Registers & Trap & Trace Devices, 515 F. Supp. 2d 325, 328 (E.D.N.Y. 2007).

[88] *Id.*; *see also* 18 U.S.C. § 3122 (2006).

[89] *In re Applications for Pen Registers*, 515 F. Supp. 2d at 336.

[90] *Id.*

[91] *In re* Applications for Historical Cell Site Info., 509 F. Supp. 2d 64 (D. Mass. 2007).

[92] *Id.* at 66; *see also* 18 U.S.C. § 2703(d) (2006).

[93] *In re Applications for Historical Cell Site Info.*, 509 F. Supp. 2d at 69.

> Court's issuance of the order. . . . it is unrealistic to believe that in the explosive world of technological advancement, the Government would not some day (if not now) be able to receive a signed order at 4:00 p.m., e-mail or fax the order to a telecommunication service provider by 4:05 p.m., and receive a cell phone's "historical" cell site information from 3:59 p.m., dramatically narrowing if not pinpointing a location. If this example is not *de jure* "real time" tracking, it is certainly *de facto* "real time" tracking.[94]

Given this fact, the court concluded that "the distinction between cell site data and information gathered by a tracking device has practically vanished"[95] and the government was required to meet the higher standard of probable cause that was statutorily required for using real-time tracking devices.[96]

Unfortunately, the kind of formalism we saw in *Olmstead* and *Smith* still appears in some modern cases. In *United States v. Scarfo*,[97] as previously discussed,[98] a district court in New Jersey was faced with the government's use of a key logger system (KLS)—software that transmitted to law enforcement every keystroke the computer user typed into his computer.[99] In order to get around the provisions of Title III, the government designed its KLS to only intercept keystrokes when the defendant's modem was turned off.[100] In this way, the government was able to intercept every piece of information the defendant typed into his computer—even information that was ultimately destined to be included in an e-mail, or information (such as a password) that would give the government access to e-mail, as long as the modem was not operational at the time the defendant typed the letters. The court accepted this clever scheme, noting that "[s]ince Scarfo's computer possessed no other means of communicating with another computer save for the modem, the KLS did not intercept any wire communications" and Title III did not apply.[101] In truth, however, this kind of ongoing, overbroad surveillance (which by its nature intercepts far more than the particular information that the government has cause to search for) is exactly the type of surveillance that Title III was meant to restrict. Thus, the KLS is functionally much more like a wiretap than it is like a traditional search, but the court only considered a narrow view of how the KLS could be classified rather than how it functioned in reality.

---

[94] *Id.* at 75 (footnote omitted).

[95] *Id.* at 70 (quoting *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 754 (S.D. Tex. 2005)) (internal quotation marks omitted).

[96] *In re Applications for Historical Cell Site Info.*, 509 F. Supp. 2d at 75-76; *see* 18 U.S.C. § 3117(b) (2006).

[97] 180 F. Supp. 2d 572 (D.N.J. 2001).

[98] *See supra* notes 65-67 and accompanying text.

[99] *Scarfo*, 180 F. Supp. 2d at 574.

[100] *Id.* at 582.

A similar example of formalism can be found in *United States v. Ropp*,[102] in which a defendant was accused of violating the Wiretap Act[103] when he placed his own version of a KLS on a victim's computer and recorded the e-mails she was typing.[104] The court concluded that the defendant had not violated the Act because the KLS recorded the e-mail *before* the victim pressed the "send" key—that is, before any "wire transmission" occurred.[105] While this may be a correct holding given the specific language found in the Wiretap Act (especially given the need to interpret criminal statutes narrowly), the *reasoning* of the *Ropp* court was troubling, since the court put great emphasis on the fact the KLS was installed on the cable that attached the victim's keyboard to her central processing unit (CPU), rather than the cable that attached the CPU to the Internet:

> [T]he communication in question is not an "electronic communication" within the meaning of the statute because it is not transmitted by a system that affects interstate or foreign commerce. The "system" involved consists of the local computer's hardware—the Central Processing Unit, hard drive and peripherals (including the keyboard)—and one or more software programs including the computer's operating system . . . and either an e-mail or other communications program being used to compose messages. Although this system is connected to a larger system—the

---

[101] *Id.* (citation omitted). The court concluded that a search warrant was sufficient. *See id.*

[102] 347 F. Supp. 2d 831 (C.D. Cal. 2004).

[103] *See* 18 U.S.C. § 2511(1)(a) (2006).

[104] *Ropp*, 347 F. Supp. 2d at 831.

[105] *Id.* at 837.

> network—which affects interstate or foreign commerce, the transmission in issue did not involve that system.[106]

The implication is that if the defendant had placed his KLS on a different cable—perhaps the one that connected the CPU to the Internet and was therefore integral to the "larger system"—he would have been guilty of violating the Wiretap Act, even though he was recording exactly the same information in almost exactly the same way.

CONCLUSION

New technology has impacted the law of surveillance regulation in significant ways. Most of these changes have been predictable and, perhaps, inevitable. It is no surprise, for example, that Congress would step in to set out its own regulations in this area, given the rapid pace of change and the occasional missteps by the courts in attempting to keep up with this pace. And since different methods of surveillance involve different levels of intrusion into individual privacy, it should be expected that the courts and Congress would set up various different standards for each of these methods. Increased congressional involvement, along with the greater dangers posed by criminals who use technology for committing their crimes, can lead to courts becoming overly deferential to the other branches of government.

These trends all seem to be destined to continue into future decades. Congress has created a comprehensive framework of statutes regulating technological surveillance, and the courts have come to rely on—and even borrow from—these statutes. The differing standards created by these statutes have been approved by the courts and even—in the case of video surveillance—transformed into constitutional requirements. Given their past record, courts are likely to continue to misunderstand how new surveillance technologies work. The good news is that Congress is ready and more than willing to step in to correct these mistakes.

---

[106] *Id.* at 837-38.

THE WARREN COURT'S HOUSE BUILT ON SAND: FROM SECURITY IN PERSONS, HOUSES, PAPERS, AND EFFECTS TO MERE REASONABLENESS IN FOURTH AMENDMENT DOCTRINE

Jack Wade Nowlin[*]

INTRODUCTION 1018
I. CONSTITUTIONAL DOCTRINE: IMPLEMENTATION, FRAMING, AND ANCHORING 1020
  A. Implementing the Fourth Amendment Through the Creation of Doctrine 1020
  B. Constitutional Doctrine and Framing Effects 1021
  C. Constitutional Doctrine and Anchoring Effects 1026
II. FROM "PERSONS, HOUSES, PAPERS, AND EFFECTS" TO "REASONABLE EXPECTATIONS OF PRIVACY" 1031
  A. Katz *and Rival Frames: "Protected Interests" Versus "Reasonable Expectations of Privacy"* 1031
  B. Kyllo, *"Houses," and Rival Frames: A Return to "Protected Interests" Within the "Reasonable Expectation of Privacy" Framework* 1041
  C. "Papers," Digital Documents, and Rival Frames: A Return to "Protected Interests" Within the "Reasonable Expectation of Privacy" Framework? 1046

---

[*] Associate Professor and Jessie D. Puckett, Jr., Lecturer in Law, The University of Mississippi School of Law. Ph.D., M.A., Princeton University; J.D., The University of Texas School of Law; B.A., Angelo State University. I was inspired to write this Article in part by the scholarship of Thomas Clancy and Morgan Cloud, and I would like to extend my thanks to both scholars for their seminal work in this area. I would also like to thank Thomas Clancy and Matthew Hall for their comments on an earlier draft of this Article. Further, I would like to thank the National Center for Justice and the Rule of Law and the National Judicial College for their support in conjunction with the Fourth Amendment Symposium. Finally, I would like to thank Michael Barbee and the editors and staff of the *Mississippi Law Journal* for their assistance with this Article.

III. FROM "SECURITY" IN PROTECTED INTERESTS TO THE "REASONABLENESS" OF POLICE CONDUCT 1051
  A. Rival Frames: "Security" Versus "Reasonableness".. 1051
  B. The "Security" Era and the Warren Court's Transition to the "Reasonableness" Era 1055
  C. The Continuing Relevance of the "Security" Frame in the Court's Decisions Today............................ 1061
IV. RE-ANCHORING THE FOURTH AMENDMENT: FROM A SUBSTANTIVE BAN ON EVIDENCE-GATHERING SEARCHES TO FACILITATING THE CONTROL OF CRIME........... 1063
  A. The Mere Evidence Rule.. 1063
  B. The Rival Frames and Evidence-Gathering Searches 1065
  C. Re-Anchoring Fourth Amendment "Reasonableness" in Crime-Control Policies.................... 1070
V. THE FUTURE OF SECURITY IN PROTECTED INTERESTS: STATUS QUO OR REFORM?.................................. 1075
CONCLUSION 1082

INTRODUCTION

In the 1960s, the Warren Court revolutionized the foundations of Fourth Amendment doctrine—shifting constitutional analysis away from a traditional concern with the security of persons, houses, papers, and effects towards an innovative analysis centered on the prohibition of unreasonable searches and seizures. The Warren Court's aim was to expand the protections of the Fourth Amendment well beyond its traditional contours, but the Court's doctrinal innovations have failed to fulfill that original promise and have actually contributed to a narrowing of the scope of the Fourth Amendment in important respects. This Article will advance a partial account of this failure emphasizing the framing and anchoring effects of the Warren Court's new doctrines. This account is offered as "one view of the cathedral" in full awareness that there are other plausible perspectives on the Warren Court's revolution and its impact on the law today.[1]

First, this Article will contend that the Warren Court's doctrinal innovations in favor of open-ended "reasonableness" analyses reframed key Fourth Amendment doctrines in ways which are not inherently suggestive of expansive protection and which are particularly vulnerable to narrow interpretations in the hands of judicial actors predisposed to embrace crime-control policies or defer to local authorities. This reframing of Fourth Amendment doctrine empowered Justices in the Nixon era and beyond to craft plausible doctrinal readings of the Fourth Amendment offering minimal protections to individual rights. Second, this Article will contend that the ultimate effect of the Warren Court's doctrinal innovations has been to facilitate an "anchoring" of the Fourth Amendment in a social vision that routinely favors the collective goal of crime prevention over individual rights. This anchoring effect is a function of (i) the Warren Court's sweeping rejection of the traditional mere evidence rule as a substantive protection prohibiting police searches for evidence of crime and (ii) the practical result of the Court's embrace of free-floating "reasonableness" doctrines easily subject to narrow crime-control interpretations. The Warren Court's re-anchoring of the Fourth Amendment has produced a substantial bias against the rights of the individual in the now predominant analysis of Fourth Amendment "reasonableness."

Part I of this Article will discuss doctrinal implementation of the Fourth Amendment and the operation of doctrinal framing and anchoring effects more generally. Part II will discuss the implications of the Warren Court's doctrinal shift from "persons, houses, papers, and effects" as "protected interests" to "reasonable expectations of privacy." Part III will discuss the significance of the doctrinal shift in analysis from Fourth Amendment "security" in enumerated interests to the "(un)reasonableness" of police conduct. Part IV will discuss the importance of the Warren Court's wholesale rejection of the "security-driven" mere evidence rule for the ultimate establishment of a revisionist crime-control understanding of Fourth Amendment "reasonableness." Part V will outline some thoughts on the future of Fourth Amendment doctrine, and it will sketch a possible pathway for doctrinal reform which respects stare decisis and the basic contours of the "reasonableness" doctrines of the Warren Court's revolution while partially reorienting those doctrines back toward an emphasis on "security" in "protected interests."

---

[1] I borrow the phrase "one view of the cathedral," in reference to Claude Monet's series of paintings of Rouen Cathedral, from the well known article on property and liability rules. *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).

I. CONSTITUTIONAL DOCTRINE: IMPLEMENTATION, FRAMING, AND ANCHORING

A. Implementing the Fourth Amendment Through the Creation of Doctrine

In recent years, scholars who study the Constitution and the Court have increasingly emphasized the relationship between the Constitution and court-created constitutional law—between the judicial interpretation of the meaning of the Constitution and the judicial construction of constitutional doctrines.[2] When the Court resolves a Fourth Amendment case, it inquires into the meaning of the Fourth Amendment, but it must also act to translate that meaning into constitutional doctrine—the rules, tests, and standards expressed in the Court's evolving precedents.[3] The purpose of these doctrines is to "implement" the Constitution in the judicial process by establishing a reasonably determinant body of constitutional law designed for practical application by courts.[4] Constitutional doctrines—such as the tiers of scrutiny in the law of equal protection—both specify abstract constitutional values and provide an important measure of legal certainty, predictability, and stability.[5]

---

[2] For a careful discussion of the interpretation-construction distinction emphasizing the institutional differences between the judicial branch and the institutional branches, see KEITH E. WHITTINGTON, CONSTITUTIONAL CONSTRUCTION: DIVIDED POWERS AND CONSTITUTIONAL MEANING (2001).

[3] *See* Richard H. Fallon, Jr., *Foreword: Implementing the Constitution*, 111 HARV. L. REV. 56 (1997).

[4] *Id.* at 61-67.

The Court crafts doctrine to reflect constitutional meaning, but the doctrine is also shaped by other concerns—such as respect for the authority of political actors, the comparative institutional competence of judicial and non-judicial actors, and the potential costs of legal uncertainty.[6] Given these latter concerns, constitutional doctrines sometimes over-enforce and sometimes under-enforce the meaning of the Constitution.[7] The conceptual space between constitutional meaning and constitutional doctrine is a function of the Court's obligation of "fidelity" to the Constitution.[8] As Richard Fallon argues, the Court must display fidelity to the meaning of individual constitutional provisions such as the Fourth Amendment, but the Court must also be faithful to Article III of the Constitution which establishes the Court's institutional mission to operationalize the Fourth Amendment within the judicial branch, a mission that requires the creation of constitutional doctrines.[9] The focus of this Article is on the Court's obligation to create implementing doctrines for Fourth Amendment rights and on the crucial framing and anchoring effects of those doctrines.

B. Constitutional Doctrine and Framing Effects

Constitutional doctrines implement constitutional meaning and in doing so they frame issues, structure analysis, and shape conclusions. One can see this process in more detail if one considers the question of the Fourth Amendment and the constitutionality of consent searches. The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."[10] Does the meaning of the Fourth Amendment encompass a prohibition of searches in cases where an individual consents to the search? The consensus view is that it does not—at least if consent is understood in the appropriate way.[11] The Court recognizes the legitimacy of consent searches,[12] and it has found no obstacle to this view in conventional methods of constitutional interpretation grounded in text, original understanding, evolving legal traditions, social ethos, and public policy.[13] Even so, the judicial implementation of the Fourth Amendment requires that one move beyond the mere interpretation of constitutional meaning to the construction of constitutional doctrines designed to specify that meaning in a more determinant form to provide guidance for judges, attorneys, police officers, and citizens. One needs a doctrine to frame the issue and outline the precise analysis to be pursued.

---

[5] *Id.*

[6] *Id.* at 66-67. On some recurrent patterns of policy argument in law, see ALLAN C. HUTCHISON, IT'S ALL IN THE GAME: A NONFOUNDATIONALIST ACCOUNT OF LAW AND ADJUDICATION (2000); Ellie Margolis, *Closing the Floodgates: Making Persuasive Policy Arguments in Appellate Briefs*, 62 MONT. L. REV. 59 (2001).

[7] Fallon, *supra* note 3, at 64-65. On judicial under-enforcement of the Constitution, see Lawrence Gene Sager, *Fair Measure: The Legal Status of Underenforced Constitutional Norms*, 91 HARV. L. REV. 1212 (1978).

[8] Fallon, *supra* note 3, at 59-60.

[9] *Id.* The Court's institutional mission derives from its self-conception under Article III as the "ultimate expositor of the constitutional text." United States v. Morrison, 529 U.S. 598, 616 n.7 (2000).

The importance of doctrine is apparent when thinking about the question of what rules to craft to operationalize the Fourth Amendment in the area of consent searches. Consider three obvious doctrinal explanations for the basic conclusion that consent searches are compatible with the Fourth Amendment.[14] First, one could contend that a consent search is constitutionally permissible because it is a "reasonable" search under the Fourth

---

[10] U.S. CONST. amend. IV.

[11] Schneckloth v. Bustamonte, 412 U.S. 218, 227 (1973) (holding that consent searches are permissible if consent is "voluntary" on the "totality of all the circumstances").

[12] *See id.*

[13] *See, e.g.*, Georgia v. Randolph, 547 U.S. 103, 143-45 (2006) (Scalia, J., dissenting) (discussing some of the interactions between the authority to consent to a search, changes over time in the law of property, and the original understanding of the Fourth Amendment). On the conventional modes of constitutional interpretation, see PHILIP BOBBITT, CONSTITUTIONAL FATE: THEORY OF THE CONSTITUTION (1982).

[14] I will discuss a fourth approach, a "security-driven" view of "reasonableness" emphasizing the need for a compelling police justification analogous to a valid warrant for an entry into the home, later in this Article. *See infra* Part III; *cf.* Marcy Strauss, *Reconstructing Consent*, 92 J. CRIM. L. & CRIMINOLOGY 211, 216 n.11 (2001) (contrasting three theories of consent—a warrant exception theory, a "reasonableness" theory, and a "reasonable expectation of privacy" theory).

Amendment.[15] The text of the Fourth Amendment does not prohibit "reasonable" searches, and one could easily conclude that a search is "reasonable" when a police officer has received valid consent to search. This view has been adopted by the Court in its more recent consent search decisions.[16] Second, one could contend that a consent search is constitutionally permissible because valid consent to a search constitutes a waiver of the Fourth Amendment right.[17] An individual is entitled to waive his or her Fourth Amendment rights if he or she chooses, and a search made after a valid waiver of those rights would not violate the Fourth Amendment. Notably, Justice Marshall advanced this view of consent searches in his dissent in *Schneckloth v. Bustamonte.*[18]

Third, one could contend that a consent search is constitutionally permissible because such a search is not in fact a technical "search" within the meaning of the Fourth Amendment.[19] The first clause of the Fourth Amendment restricts "unreasonable searches and seizures," and its protections apply only when governmental action constitutes a Fourth Amendment search or seizure.[20] The Court has held in recent decades that only a governmental invasion of a "reasonable expectation of privacy" constitutes a "search" within the meaning of the Fourth Amendment.[21] Governmental observation of something sufficiently "expose[d] to the public" is not a "search."[22] One could easily conclude that consent to a search is a kind of public "exposure" eliminating any "reasonable expectation of privacy" and therefore the consent search is not a technical "search" under the Fourth Amendment. On this view, valid consent to a search of a container such as a suitcase eliminates the privacy in the container and its contents—just as does opening the container and dumping out its contents in plain view of the officers. Justice Marshall also advanced a similar view in dissent in *Illinois v. Rodriguez*.[23]

---

[15] Illinois v. Rodriguez, 497 U.S. 177, 186 (1990).

[16] *Id.* (holding that a search is reasonable within the meaning of the Fourth Amendment if it is based upon a reasonable appearance of authority to consent).

[17] Schneckloth v. Bustamonte, 412 U.S. 218, 278-79 (1973) (Marshall, J., dissenting).

[18] *Id.*

[19] *Rodriguez*, 497 U.S. at 189-90 (Marshall, J., dissenting).

[20] U.S. CONST. amend. IV.

[21] Katz v. United States, 389 U.S. 347, 350 (1967).

[22] *Id.* at 351.

Each of these doctrinal explanations has what can be called a "framing effect." A framing effect can be defined here in simple terms as the effect that framing or posing a given question in one way rather than another can have on our attitudes in response to the question.[24] For instance, studies have shown that responses to questions are often shaped by how the questions are put, and the framing effect can be as simple as, say, stating the anticipated consequences of a medical procedure positively (e.g., an 80% chance of survival) or negatively (e.g., a 20% chance of death).[25] A positive framing of the question in this example might increase support for the procedure while a negative framing of the question could decrease support.[26] The three doctrinal approaches to consent searches outlined above each frame the basic legal issue in a slightly different way: a consent search is permissible because it is reasonable for an officer to search with consent; a consent search is permissible because consent is a waiver of the Fourth Amendment; and a consent search is permissible because a consent search is not a Fourth Amendment search. Each explanation therefore has an at least somewhat different possible framing effect which shapes the legal analysis and conclusions that follow from the doctrine's frame.

Consider here the framing effect the approaches above have on the question of what legal test one should use to determine what counts as valid consent for a consent search—the next logical step in establishing a set of consent search doctrines to operationalize the Fourth Amendment in this area. Clearly the analysis at this step will be influenced by the initial doctrinal explanation concerning why one thinks consent searches conform to the Fourth Amendment. Each approach frames the consent search issue in a different way that has likely consequences for the next step in analysis.

---

[23] *Rodriguez*, 497 U.S. at 189-90 (Marshall, J., dissenting).

[24] For a nice discussion of framing effects generally, see WARD FARNSWORTH, THE LEGAL ANALYST: A TOOLKIT FOR THINKING ABOUT THE LAW 224-29 (2007).

[25] *Id.* at 228.

[26] *Id.*

For instance, if a consent search is framed as a "reasonable" search, doctrinal emphasis is placed on the "reasonableness" of police action. That in turn suggests that the doctrine governing "valid" consent would likely gravitate toward a "reasonableness" standard centered on the objective actions of the police. On this view, one might ask the question whether the police behaved "reasonably" in obtaining consent to search—by refraining from coercion or other "overreaching" behaviors such as exploiting a known weakness of the suspect.[27] Similarly, if consent is framed as a Fourth Amendment waiver, doctrinal emphasis is placed not on the "reasonableness" of the police conduct but on whether the suspect actually waived his or her rights. That suggests in turn that the doctrine governing the "validity" of consent is a subjective standard centered on the suspect and his or her mental state—whether the suspect in fact intended to waive his or her Fourth Amendment rights and whether any waiver was sufficiently informed by an understanding of its legal consequences. On this view, one might then ask a standard waiver question common in many areas of criminal procedures: Was the suspect's consent-as-a-waiver in fact knowing, intelligent, and voluntary?[28]

Clearly, these two rival approaches to the "validity" of consent could generate quite different conclusions in, say, a case in which police do not engage in any objectively "unreasonable" coercion but in which a defendant's subjective consent is less than knowing and intelligent. Of course, recognition of these different outcomes often drives an initial preference for one doctrinal frame ("a consent search is permissible if the search is reasonable") over another ("a consent search is permissible if the consent is a valid waiver"). Since the doctrinal framing of the issue affects later analysis and conclusions, an upfront recognition of those effects may drive the decision on how to frame an issue doctrinally. Not surprisingly, these concerns appear to have motivated, in part, the choice of doctrinal frame by the majority and dissenting opinions in *Schneckloth*.[29]

---

[27] *Cf.* Colorado v. Connelly, 479 U.S. 157, 167 (1986) (holding that under the Due Process Clause "coercive" behavior by police is a necessary predicate to finding that a confession is not 'voluntary'); Schneckloth v. Bustamonte, 412 U.S. 218, 227 (1973) (holding that a search is permissible under the Fourth Amendment if consent is given "voluntarily" under the "totality of all the circumstances").

[28] *See Schneckloth*, 412 U.S. at 277 (Marshall, J., dissenting); Johnson v. Zerbst, 304 U.S. 458, 464 (1938) (stating that a waiver of a constitutional right is "ordinarily an intentional relinquishment . . . of a known right").

C. Constitutional Doctrine and Anchoring Effects

The crafting of constitutional doctrines also has important anchoring effects on later decision making. An "anchoring effect" can be defined simply as the influence that an initial "anchor" (e.g., a piece of information, a value judgment, a monetary demand, a decision, etc.) can have on later judgments.[30] Anchoring, a function of human psychology, is a cognitive bias in which the anchor, as an initial reference point for decision, exercises an influence analogous to "gravitational pull" on the ultimate judgment of decision makers.[31] The effect of an anchor can be strong even when decision makers are aware of the effect and are consciously resisting the anchor.[32] For example, studies have shown that initial monetary demands in negotiations, whether low or high, tend to have a substantial effect on the final outcome of the negotiations—even when experienced negotiators are involved.[33] Advisory standards, such as the Federal Sentencing Guidelines, can have significant anchoring effects, and the Sentencing Guidelines have likely influenced sentencing upwards or downwards "even when the sentence falls outside the

---

[29] The main point of contention in *Schneckloth* was whether the state must prove that consent is "knowing and intelligent" in order for a search on the basis of consent to comply with the Fourth Amendment. *Schneckloth*, 412 U.S. at 235-58. The waiver theory of consent offered by the dissent tends to support a "knowing and intelligent" consent requirement, and the majority appears to have been unwilling to endorse the waiver view in part because it wished to avoid the burdens on law enforcement which that view would appear to entail. *Id.*

[30] For a nice discussion of anchoring effects generally, see FARNSWORTH, *supra* note 24, at 230-36.

[31] *Id.*

[32] *Id.*

[33] *Id.*

[Guidelines] range"[34] because they "provide a crucial "starting point or 'anchor' for judges" in determining a sentence.[35]

A decision establishing a given legal doctrine can also have an anchoring effect on later decision makers, who will take the status quo as their point of departure (even when they ultimately decide to change it) and who may also have internalized or at least acclimated to that status quo. There is good reason to think that judicial actors in common-law systems are especially susceptible to the anchoring effect of prior judicial decisions given the value common-law systems place on adherence to precedent, a value which is reflected in the formal doctrine of stare decisis.[36] A judicial decision establishing a particular doctrinal frame ("a consent search is permissible if the search is reasonable") as a precedent exercises not only a framing effect but may also have a substantial anchoring effect on the judgments of later judicial actors—whose views will be shaped in some respects by the presence of the doctrinal frame.

Georgia v. Randolph, a recent consent search case, illustrates the likely anchoring effects of precedent.[37] The issue in *Randolph* was the reasonableness of the police search of a residence when one co-tenant consented to the search but another co-tenant was present and objected to the search.[38] The Court held by a 5-3 vote that police searches in such circumstances are unreasonable because "widely shared social expectations" suggest that a private visitor would not enter a home under the same circumstances.[39]

---

[34] Recent Case, *Criminal Law—Sentencing Guidelines—Second Circuit Holds That Imposing Below-Guidelines Sentence Using Retroactive Guidelines Range Increase Does Not Violate Ex Post Facto Clause*, 124 HARV. L. REV. 2091, 2094-95 (2011).

[35] *Id.* at 2095 (quoting United States v. Turner, 548 F.3d 1094, 1099 (D.C. Cir. 2008)). This anchoring effect can present an ex post facto issue arising when an upward alteration in the Sentencing Guidelines range—occurring after a defendant's criminal conduct—has an anchoring effect which operates retroactively to increase the defendant's sentence, an effect which could be obscured by the fact that the ultimate sentence still falls below the formal range increase even though it is higher than it would have been without the anchoring effect of the range increase. *See id.*

[36] On the doctrine of stare decisis, see Burnet v. Coronado Oil & Gas Co., 285 U.S. 393, 405-06 (1932) (Brandeis, J., dissenting).

[37] 547 U.S. 103 (2006).

[38] *Id.* at 106.

[39] *Id.* at 111.

Since "no sensible [private] person would go inside" when a co-tenant is present and objects to their entry, a search by police in those circumstances is unreasonable under the Fourth Amendment.[40] The dissent, by contrast, asserted that an approach centered on "shared social expectations" is too amorphous and uncertain in application to serve as a constitutional standard given the almost infinite variety of differing social circumstances, and advocated instead adoption of a bright-line rule turning on the shared authority co-tenants have over their common home.[41]

For the purposes of this Article, what is notable about *Randolph* is simply that all the Justices viewed the issue as one centering on the interpretation of the contours of the consent search doctrines established by cases such as *Schneckloth v. Bustamonte*[42] and *United States v. Matlock*,[43] the first co-tenant consent search case. Both of those decisions included firm dissenting opinions advocating an analysis centered on the question of knowing and intelligent waiver,[44] which were ignored by the Justices in *Randolph*. The consent search question in the Georgia case was both framed by these precedents ("a consent search is permissible if the search is reasonable") and anchored by them as a practical matter—the Justices made no effort to revisit and reformulate the foundations of Fourth Amendment consent search doctrine but rather took the established doctrines as a starting point for their analysis.

Of course, it is conceivable that all the Justices simply agreed with this approach in some fashion wholly independent of the earlier cases, but no actual defense of the "reasonableness" approach over other approaches was advanced by any Justice. Given the substantial number of dissenting Justices in these early cases,[45] and the range of plausible doctrinal explanations for consent searches,[46] it seems likely that the views of the *Randolph* Justices were simply canalized by the early decisions both as a formal matter of stare decisis and perhaps in nonformalized ways as well. In sum, the anchoring effect of the earlier decisions on consent likely played a significant role in determining the frame that structured all the Justices' analyses in *Randolph*.

---

[40] *Id.* at 113.

[41] *Id.* at 127-42 (Roberts, C.J., dissenting).

[42] 412 U.S. 218 (1973).

[43] 415 U.S. 164 (1974).

[44] *Matlock*, 415 U.S. at 188 (Brennan, J., dissenting); *Schneckloth*, 412 U.S. at 277 (Marshall, J., dissenting).

[45] The same three Justices—Douglas, Brennan, and Marshall—dissented in both cases. *Matlock*, 415 U.S. at 178, 188; *Schneckloth*, 412 U.S. at 275-77.

Also important are the broader effects of doctrinal anchoring—especially the influence that implementing doctrines can have over time on the way the general legal community comes to think about the original constitutional provision at issue. "We are under a Constitution, but the Constitution is what the judges say it is," Chief Justice Hughes once famously observed.[47] That statement is best understood not as an expression of constitutional cynicism but of constitutional realism: In a legal system where the Court has the final say on the meaning of the Constitution,[48] the practical effect of most constitutional provisions will turn on the doctrines created by the Court. Those who are most concerned with the real-world effect of the Constitution will therefore study court-created constitutional doctrine more than constitutional theory or history.[49] The end result is that the distinction between the Constitution and court-created constitutional law, obscure to begin with, becomes blurred even further in practice.

Lower court judges, lawyers, and police officers are by necessity concerned with the practical application of the Fourth

---

[46] *See supra* Part I.B.

[47] CHARLES EVANS HUGHES, ADDRESSES OF CHARLES EVANS HUGHES, 1906-1916 at 185 (2d ed. 1916).

[48] United States v. Nixon, 418 U.S. 683, 703 (1974); Cooper v. Aaron, 358 U.S. 1, 18 (1958).

[49] This is often true even for arguments addressed to the Supreme Court. For instance, Charles Fried, who served as Solicitor General in the Reagan Administration, states that a good legal brief addressed to the Court is "largely analogy and precedent" and that he "tease[d] the lawyers in [his] office that the ideal SG's brief would have not one word that is not in quotations marks and attributed to some prior Supreme Court opinion." CHARLES FRIED, ORDER AND LAW: ARGUING THE REAGAN REVOLUTION—A FIRSTHAND ACCOUNT 66 (1991); *cf.* Karl N. Llewellyn, *A Realistic Jurisprudence—The Next Step*, 30 COLUM. L. REV. 431 (1930) (advocating the study of the practical "working" rules that capture the actual conduct of government officials over the study of the abstract "paper" rules found in judicial opinions and statutes).

Amendment and thus with the doctrinal construction of the Fourth Amendment established by the Court. For these actors, the Fourth Amendment as a provision of the Constitution is first and foremost embodied in a set of judicially-crafted constitutional doctrines. Some of these actors will in fact internalize Fourth Amendment doctrines and view the doctrines as the "meaning" of the amendment. Others who do not internalize the doctrines will tend at least to acclimate to them—accepting the established doctrines as the binding law and becoming accustomed to them as the operational rules that govern cases. By processes of internalization and acclimation, a decision that might have been viewed as outrageous on the day it was decided can seem a few years later like a mere mistake which should be respected as a matter of precedent and—after a few years more—like a perfectly reasonable and perhaps even correct view of the Fourth Amendment.

The Court's doctrines shape how later Justices and the broader legal community view the Fourth Amendment even as the Court's view of the Fourth Amendment influences the crafting of Fourth Amendment doctrines. Thus, the perceived meaning of the Fourth Amendment shapes attitudes towards the doctrine, but doctrinal anchoring effects—both informal effects and the formal effects associated with stare decisis—also shape perceptions of the Fourth Amendment. This process can act as a form of feedback loop so that a "new normal" of Fourth Amendment doctrinal innovation in one era can so shape the view of the Fourth Amendment that to a later generation the innovative doctrines seem quite natural and in some cases appear almost axiomatically correct. The fact that so many Americans have a healthy faith in progress over time simply reinforces the view that newer doctrines are likely to be improvements over older ones, even as the newer doctrines themselves become the "dead hand" of the past for the next generation.

This Article will contend in the next three parts that the Warren Court's reframing and anchoring of the Fourth Amendment in innovative doctrines has undermined the amendment's basic protections in important respects. Of course, the framing and anchoring effects of these doctrines can also predispose one to view them with more complacency than one otherwise might, and may well obscure the full import of their contraction of Fourth Amendment rights. With these thoughts in mind, this Article now turns to an examination of the Warren Court's Fourth Amendment revolution.

II. FROM "PERSONS, HOUSES, PAPERS, AND EFFECTS" TO "REASONABLE EXPECTATIONS OF PRIVACY"

A. Katz *and Rival Frames: "Protected Interests" Versus "Reasonable Expectations of Privacy"*

What governmental actions trigger the basic protections of the Fourth Amendment—such as the requirement of a warrant based upon probable cause? This is a foundational question, and it places a constitutional decision maker at a doctrinal crossroads. The Supreme Court in confronting this question has had to choose implementing doctrines which carry inevitable framing and anchoring effects. The Court has had to decide how to frame the inquiry and which text, which concepts, which values will be emphasized in the doctrinal construction—and which will not.

Consider a set of facts based upon those of the Court's landmark decision in *Katz v. United States*, a case which addressed these doctrinal questions and which represents a profound shift in the Court's analysis.[50] Police place a tap on the telephone wires on the outside of a telephone booth and listen in on the telephone conservation which occurs within the booth.[51] Does this investigative act trigger the protections of the Fourth Amendment which would presumptively require police to obtain a warrant to conduct the surveillance? What doctrinal approach should one take here?

One can contrast here two rival ways to frame the doctrinal view—both embraced more-or-less by the Court at different points in time. The older view can be called the "protected interest" view.[52] This traditional approach emphasized the interests specifically enumerated as protected in the text of the Fourth Amendment, "persons, houses, papers, and effects," and the common-law principles rooted in property law that formed the important broader legal context of the text.[53] The newer view, which the Court adopted in the 1960s, can be called the "reasonable expectation of privacy" view.[54] This newer approach emphasizes the textual reference to "searches" in the Fourth Amendment, and it defines a "search" doctrinally as a governmental invasion of a "reasonable expectation of privacy."[55] The two rival frames thus emphasize (i) different parts of the Fourth Amendment text ("persons, houses, papers, and effects" versus "searches and seizures") and (ii) different forms of legal analysis (common-law legal traditions versus an open-ended "reasonableness" test).

---

[50] Katz v. United States, 389 U.S. 347 (1967).

[51] *Id.* at 348.

[52] For a comprehensive account of the concept of "protected interests" in Supreme Court doctrine over the course of Fourth Amendment history, see Thomas K. Clancy,

Consider two well-known applications of the Court's traditional "protected interest" approach. In 1924, the Court, in *Hester v. United States*, held that a police search of an "open field" does not implicate the Fourth Amendment because an "open field" is not a "person, house, paper, or effect" protected by the amendment.[56] Justice Holmes observed—in a brief opinion for a unanimous Court—that the legal distinction between a "house" and an "open field" is "as old as the common law" itself and thus that the protection afforded "houses" in the Fourth Amendment is not extended to "open fields."[57] In 1928, the Court, in *Olmstead v. United States*, held that a wiretap of a defendant's telephone involving the wires outside of his home did not implicate the Fourth Amendment.[58] The Court reasoned that the "construction" of the Fourth Amendment favored by the Court could not "justify enlargement of the [its] language . . . beyond the possible practical

---

What Does the Fourth Amendment Protect: Property, Privacy, or Security?, 33 WAKE FOREST L. REV. 307 (1998).

[53] *See id.* at 309-27.

[54] *See id.* at 327-39.

[55] *Katz*, 389 U.S. at 350.

[56] 265 U.S. 57, 59 (1924).

[57] *Id.*

[58] 277 U.S. 438, 464 (1928).

meaning of houses, persons, papers, and effects" to extend to wires "stretched" along "highways" outside of the home.[59]

The traditional "protected interest" view had both a "strict" and a "liberal" expression, the latter tracing its roots back to the Court's landmark decision in *Boyd v. United States* in 1886.[60] The Court in both *Hester* and *Olmstead* adhered to a "strict" construction of "protected interests" which limited those interests to the dimensions established by their original basis in common-law property rights.[61] The "liberal" construction, by contrast, invoked property rights as the foundation for a broader view of the Fourth Amendment, one which built on a property rights base but which was willing to extend Fourth Amendment protections beyond that base.[62] Justice Butler, dissenting in *Olmstead*, endorsed the latter position.[63] In his dissent, Justice Butler advocated extending the traditional protections of the Fourth Amendment to wiretaps outside of homes on the "liberal" theory that the "Fourth Amendment safeguards against all evils that are like and equivalent to those embraced within the ordinary meaning of its words."[64] A phone tap, on this view, is an "evil" equivalent to, say, an actual incursion into the home by government agents to eavesdrop or rifle through private papers, and thus it is equally violative of the Fourth Amendment.

Significantly, a majority of the Court embraced a "liberal" construction of the Fourth Amendment in *Silverman v. United States*.[65] The Court in *Silverman* recognized that homes and offices are constitutionally protected areas within the ambit of the meaning of the word "house" in the Fourth Amendment, and the Court held that Fourth Amendment "houses" are protected against actual physical intrusions by the government even when the intrusions do not constitute a technical trespass under property law—thus broadening the protections of the traditional common-law approach beyond strict trespass analysis.[66] On this view, the government's actual physical invasion into a house—even though not technically a trespass—sufficiently compromised the security of the house to warrant the protections of the Fourth Amendment. On these grounds, the Court recognized a distinction between police use of a "spike mike" listening device which involved an actual physical intrusion into a house and the use of a "detectaphone" which did not.[67]

---

[59] *Id.* at 465.

[60] 116 U.S. 616, 635 (1886) (stating that "constitutional provisions for the security of person and property should be *liberally* construed" because "[a] close and literal construction deprives them of half their efficacy, and leads to gradual depreciation of the right, as if it consisted more in sound than in substance" (emphasis added)).

[61] Notably, the Court in *Olmstead* characterized its own approach as a "liberal" construction. *Olmstead*, 277 U.S. at 465. Its approach, however, is certainly "strict" in comparison to the *Olmstead* dissents.

[62] *See id.* at 485 (Butler, J., dissenting).

[63] *Id.*

[64] *Id.* at 488.

[65] 365 U.S. 505 (1961).

As for our initial hypothetical case concerning the tap of a telephone booth based on the facts of *Katz*, if a court were to analyze the issues under the "protected interest" approach, it might focus on the Fourth Amendment text concerning "houses" as a "protected interest."[68] Given that focus, a court would ask two basic questions: (i) whether a telephone booth falls within the category of "houses" enumerated in the Fourth Amendment as constitutionally protected areas; and, if so, (ii) whether a police wiretap compromises the security of the telephone booth so as to trigger the protections of the Fourth Amendment—by either a common law trespass, a physical intrusion, or an "equivalent evil" such as the use of a technological device as a substitute for a trespass or intrusion.

On the first issue, a court might conclude that a telephone booth is a kind of "house" as enumerated in the Fourth Amendment and thus that a telephone booth is a constitutionally protected area. Why? Because a telephone booth is a building with a roof atop four walls; it is designed to protect privacy in telephone conservations; and it is in effect "rented" for privacy purposes for a few minutes at a time by paying to make a telephone call.[69]

---

[66] *Id.* at 511.

[67] *Id.* at 512.

[68] Under a "liberal" construction of the "protected interest" view, other possible points of focus would be on the telephone conversation as an electronic equivalent of "papers" or as an extension of the "person."

[69] *Cf.* Katz v. United States, 389 U.S. 347, 352 (1967) (stating "[o]ne who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to

Conversely, a court might conclude that a telephone booth is not a "house" within the meaning of the Fourth Amendment perhaps because the booth has transparent walls, is not designed for an overnight stay, and overall has minimal privacy protections.[70]

Second, if a court concluded that a telephone booth is a constitutionally protected area, it might next conclude that the wiretap compromises the security of the telephone booth under a "liberal" construction of the Fourth Amendment. A court might reach this conclusion by viewing the wiretap as simply the technological equivalent of a trespass or physical invasion—given that wiretap technology allows the government to obtain information it could have obtained under the technological limits of the founding era only by more intrusive means.[71] Or a court might conclude the reverse under a stricter construction of the Fourth Amendment: The security in the telephone booth is compromised only by a technical trespass or actual physical intrusion,[72] and Fourth Amendment security is simply subject to some erosion with the advent of new technologies.[73] In short, the case could have come out either way under a "protected interest" analysis.

In *Katz*, the parties expected the Court to follow the traditional "protected interest" view and, not surprisingly, the

---

place a call is surely entitled to assume that the words he utters . . . will not be broadcast to the world").

[70] *See id.* (noting the government's argument that there is no "reasonable expectation of privacy" in a telephone booth because of its transparent walls).

[71] *Cf.* Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding that government use of a sense-enhancement device not in general public to explore details of a home that could not have been discovered at the time of the framing without an actual physical intrusion is a search within the meaning of the Fourth Amendment); Olmstead v. United States, 277 U.S. 438, 485 (1928) (Butler, J., dissenting). On the similarities between Justice Butler's dissent in *Olmstead* and the opinion of the Court in *Kyllo*, see Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 MISS. L.J. 5, 46 (2002).

[72] *Cf. Silverman*, 365 U.S. at 512 (holding that an actual physical invasion of a constitutionally protected area is required to trigger the protections of the Fourth Amendment).

[73] *Cf. Kyllo*, 533 U.S. at 34 (stating the Fourth Amendment must be interpreted to limit governmental use of new technologies to preserve the degree of privacy in the home against the government that existed when the amendment was adopted). The Court does note in *Kyllo* that once the technologies are in "general public use" their use by police does not constitute a Fourth Amendment "search." *Id.* at 40.

petitioner formulated the dispute in light of the Court's traditional approach in cases such as *Silverman*. This formulation centered on the textual statement of protected interests and the principles of the common law: (i) "[w]hether a public telephone booth is a constitutionally protected area" under the Fourth Amendment and (ii) "[w]hether physical penetration of a constitutionally protected area" is required to trigger the protections of the Fourth Amendment.[74] The Court, however, did not adhere to the traditional approach. Instead, the Court called the traditional formulation of the issues "misleading."[75]

The Court in *Katz* rejected the traditional approach and framed a new approach to the threshold question of whether the protections of the Fourth Amendment apply. This new approach emphasized the Fourth Amendment's textual reference to "searches" and centered on an open-ended "reasonableness" test used by the Court to define when a "search" occurs under the Fourth Amendment.[76] On this new view, police engage in a Fourth Amendment "search" triggering the protections of the amendment when they invade a "reasonable expectation of privacy."[77] As a result, the Court asserted in *Katz* that the operative question was whether Katz had a "reasonable expectation" with respect to the privacy of his conversation within the telephone booth.[78] If Katz had a "reasonable expectation of privacy" within the telephone booth, then an invasion of that expectation with a listening device was a "search" triggering the protections of the Fourth Amendment—even without an actual physical invasion of the interior of the booth or a determination that a phone booth was a protected area.[79] On the other hand, if Katz did not have a "reasonable expectation of privacy" within the telephone booth, then no search occurred and no Fourth Amendment protections applied.

---

[74] *Katz*, 389 U.S. at 349-50.

[75] *Id.* at 351.

[76] *Id.* at 353.

[77] *Id.*

[78] Justice Stewart in *Katz* principally uses the word "justifiable" to refer to Katz's expectation of privacy. *Id.* The phrase "reasonable expectation of privacy" derives from Justice Harlan's concurrence. *Id.* at 360 (Harlan, J., concurring). This "reasonableness" formulation of the *Katz* test is now more common. *See Kyllo*, 533 U.S. at 32-33; Clancy, *supra* note 52, at 328.

[79] *Katz*, 389 U.S. at 348-54.

On this question, the Court decided that Katz's expectation of privacy was "reasonable" because "[o]ne who occupies a [telephone booth], shuts the door behind him, and pays the toll," is "entitled to assume that the words he utters . . . will not be broadcast to the world" and that for the Court "[t]o read the Constitution more narrowly [would be] to ignore the vital role that the public telephone has come to play in private communication."[80] The Court concluded that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth."[81] Since the police wiretap invaded a "reasonable expectation of privacy," it constituted a "search" within the meaning of the Fourth Amendment, and it presumptively required a warrant.[82]

Notably, the application of the "reasonable expectation of privacy" approach to the facts of *Katz* is far from obvious. The Court concluded that Katz had a "reasonable expectation of privacy" because the purpose of a telephone booth is to provide privacy for telephone conversations[83] and because of the important role that telephone booths played in contemporary life in the 1960s.[84] The Court, however, could have concluded that Katz did not have a "reasonable expectation of privacy" in the booth if it had emphasized other potential factors—such as the glass walls of the telephone booth exposing Katz to visual observation,[85] the fact that a telephone operator could have listened in on the call,[86] or that the party on the other end of the conversation could have shared the conversation with others by transmitting the conversation, or recording it, or simply repeating its content.[87] The new *Katz* analysis, given its open-ended "reasonableness" analysis, cannot assure the protection of privacy in a telephone booth.

---

[80] *Id.* at 352.

[81] *Id.* at 353.

[82] *Id.* at 354-59.

[83] *Id.* at 352.

[84] *Id.*

[85] The government raised this point in *Katz*. *Id.* If the government could have obtained the substance of Katz's conversation through the glass walls of the phone booth by visual observation, say, through reading Katz's lips, then there is a plausible argument that no Katzian "reasonable expectation of privacy" existed in the conversation. *Cf.* United States v. Knotts, 460 U.S. 276, 282 (1983) (holding that use of an electronic device to track the location of a vehicle on public roadways is not a search within the meaning of the Fourth Amendment because police could have obtained the information by direct visual observation).

For purposes of this Article, what is important about *Katz* is the profound doctrinal reframing it embraced—from a focus on "persons, houses, papers, and effects" informed by long-standing common-law traditions to a focus on the word "search" defined by a flexible analysis of "reasonable expectations of privacy."[88] The obvious reason behind the reframing in *Katz* was to expand the reach of the Fourth Amendment beyond its enumerated interests: persons, houses, papers, and effects.[89] However, the Katzian "reasonable expectation of privacy" approach has not delivered on that promise and it in fact has threatened to undermine the Fourth Amendment's traditional protections.

The Court, more than four decades after *Katz*, has not used the "reasonable expectation of privacy" doctrine to expand the reach of the Fourth Amendment beyond a point where the "protected interest" doctrine could also have gone.[90] Consider *Oliver*,[91] the Katzian follow up to *Hester*,[92] the original case which held that an "open field" is not protected by the Fourth Amendment because it is not a person, house, paper, or effect.[93] In *Oliver*, the Court held that the search of an "open field" is not a "search" within the meaning of the Fourth Amendment in part because there is no "reasonable expectation of privacy" in an open field, given the typical uses of "open fields" for agricultural or other utilitarian purposes rather than for privacy-intensive purposes.[94]

---

[86] *Cf.* Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding that one has no "reasonable expectation of privacy" in the telephone numbers one dials because this information is knowingly "exposed" to the telephone company and one "assume[s] the risk" that the telephone company will turn the information over to police). On the tension between *Smith* and *Katz*, see *id.* at 746-48 (Stewart, J., dissenting).

[87] *Cf.* United States v. White, 401 U.S. 745, 752 (1971) (holding that police use of a "false-friend" to record or transmit a conversation does not constitute a "search" within the meaning of the Fourth Amendment).

[88] *See* Clancy, *supra* note 52, at 320-29.

[89] *Id.*

[90] *Id.* at 329-40; Cloud, *supra* note 71, at 7.

[91] Oliver v. United States, 466 U.S. 170 (1984).

[92] Hester v. United States, 265 U.S. 57 (1924).

[93] *Id.* at 59.

Consider also *California v. Ciraolo*,[95] a case involving police use of an aircraft to observe the curtilage of a home.[96] Under the "protected interest" view, the common law establishes that curtilage is an extension of the home entitled to Fourth Amendment protection,[97] and the pivotal issue would be whether an actual physical intrusion is necessary to consider the security of the curtilage compromised. This question could easily go either way depending on whether one held strictly to a physical invasion approach to security or "liberally" adjusted the standard to include functional equivalents of physical invasions enabled by technological advances.[98] Under the "reasonable expectation of privacy" view, the Court in *Ciraolo* held that there is no "reasonable expectation of privacy" in curtilage from aerial observation given that the curtilage is "knowingly exposed" to airplanes flying within a "lawful vantage point."[99]

The *Katz* Court's reframing of the Fourth Amendment in favor of a flexible test that would allow the judiciary to expand the reach of the amendment has also threatened to narrow it, especially with respect to the traditional protections for houses and papers. This is so for several related reasons. First, the *Katz* doctrine's flexible "reasonableness" test encourages policy-oriented decision making, which can just as easily restrict the reach of the Fourth Amendment as expand it—depending upon the inclination of the judges who must interpret it.[100] Thus, the original Katzian promise of a more expansive Fourth Amendment carries with it the concomitant hazard of a narrower amendment interpreted by judges who favor a crime-control view of the Fourth Amendment.[101]

---

[94] *Oliver*, 466 U.S. at 177-81. The Court in *Oliver* also stated that "*Katz*' 'reasonable expectation of privacy' standard did not sever Fourth Amendment doctrine from the Amendment's language." *Id.* at 176 n.6.

[95] 476 U.S. 207 (1986).

[96] *Id.* at 209.

[97] *Hester*, 265 U.S. at 57.

[98] *See supra* notes 65-73 and accompanying text.

[99] *Ciraolo*, 476 U.S. at 213-16.

[100] Morgan Cloud, *A Liberal House Divided: How the Warren Court Dismantled the Fourth Amendment*, 3 OHIO ST. J. CRIM. L. 33, 34 (2005); Clancy, *supra* note 52, at 339-40.

Second, the *Katz* doctrine takes the emphasis off the specific language of "persons, houses, papers, and effects" and thereby reduces the significance of this concrete enumeration of interests worthy of special protection under the amendment. The shift in emphasis away from this text has an inevitable tendency to undermine the significance of the protections afforded by the textual specification of protected interests. Third, the Katzian approach also reduces the importance of the common-law background principles which inform the understanding of the security of protected interests—such as homes and papers. This shift also undermines a source which can provide a crucial "floor" of traditional legal protection in many cases.[102]

Fourth, the new doctrinal frame also pushes the protection of houses to the margins of doctrinal analysis. As *Katz* makes clear, whether a structure such as a telephone booth is protected by the Fourth Amendment has no direct analytical connection to whether the structure is analogous to a house. The older doctrine would have reaffirmed the centrality of privacy in homes by building its doctrinal analysis of structures such as telephone booths on the ways in which they are (or are not) like houses. Whether or not a court applying this analysis decided that the structure was a kind of "house" for Fourth Amendment purposes, the substance of its analysis would have reaffirmed the importance of houses as concrete protected interests and elaborated on the ultimate policy foundation of the special protections for houses in a way that could deepen judicial appreciation of their importance. This same basic point will likely hold true for physical papers and digital documents.[103]

Finally, the Court in *Katz* stated baldly that the Fourth Amendment protects "people, not places."[104] This proposition is either meaningless (since, of course, no one claims that places have Fourth Amendment rights) or it inevitably undercuts the protection the Fourth Amendment specifically enumerates for "houses" as a constitutionally protected "place" in which "people" have a right to be "secure." Denigrating the Fourth Amendment's clear application to places *as places* will inevitably tend to erode respect for the constitutional protections afforded to those places.

---

[101] Cloud, *supra* note 100, at 72.

[102] *Id.*

[103] *See* discussion *infra* notes 142, 144 and accompanying text.

[104] Katz v. United States, 389 U.S. 347, 351 (1967).

B. Kyllo, *"Houses," and Rival Frames: A Return to "Protected Interests" Within the "Reasonable Expectation of Privacy" Framework*

Some of the conceptual fallout from *Katz*'s reframing of the Fourth Amendment—eroding security in houses—is on display in the opinions in *Kyllo v. United States.*[105] This case involved police use—without a warrant—of a thermal-imaging device to measure the heat generated inside a home to determine whether heat lamps were being used to grow marijuana.[106] The Court held 5-4 that police use of a thermal imager to monitor the heat levels in a home is a "search" that triggers the protections of the Fourth Amendment and presumptively requires a warrant.[107] The dissent concluded that the use of the thermal imager is not a search and thus would have allowed the use of a thermal imager without a warrant.[108] Both the majority opinion and the dissent demonstrate the threat the Katzian approach poses to a broad view of the Fourth Amendment.

The most thoroughly Katzian opinion in *Kyllo* is the dissent. Written by Justice Stevens and joined by three other Justices—Rehnquist, O'Connor, and Kennedy—the dissent applied the *Katz* "reasonable expectation of privacy" test in a straightforward manner consistent with the flexibility of its "reasonableness" standard. Justice Stevens summarily dismissed the claim that Kyllo had a reasonable expectation of privacy in the heat levels in his home by characterizing the privacy claim as one concerning external heat emissions.[109] "[T]he notion," Justice Stevens pronounced, "that heat emissions from the outside of a dwelling are a private matter implicating the protections of the Fourth Amendment . . . is not only unprecedented but also quite difficult to take seriously."[110] Why? Because "[h]eat waves," Justice Stevens argued, "like aromas that are generated in a kitchen . . . enter the public domain if and when they leave a building" and thus any "expectation" they will "remain private" is "implausible" and unreasonable.[111]

---

[105] Kyllo v. United States, 533 U.S. 27 (2001).

[106] *Id.*

[107] *Id.*

[108] *Id.* at 41 (Stevens, J., dissenting).

[109] *Id.* at 42.

Significantly, Justice Stevens also invoked the "strong public interest" in clearly recognizing governmental authority to monitor "emission from homes" in cases involving "smoke, suspicious odors, odorless gases, airborne particulates, or radioactive emissions, any of which could identify hazards to the community."[112] This last point suggests that concern for facilitating effective law enforcement is relevant to the Fourth Amendment's "reasonable expectation" inquiry. Justice Stevens thus concluded that the use of the thermal imager is not a search within the meaning of the Fourth Amendment and police were not required to obtain a warrant to use an imager to monitor heat levels in Kyllo's home.[113]

Justice Scalia's opinion for the Court concluded that Kyllo's home was protected from police use of a thermal imager without a warrant.[114] The majority opinion was decidedly less Katzian in substance than the dissent, and its quiet but dramatic retreat from *Katz* also illustrates the problems with the *Katz* approach. Justice Scalia first criticized the *Katz* "reasonable expectation of privacy" approach and then purported to apply it while actually embracing the core of the substance of the traditional "protected interest" approach discarded by the Court decades earlier.[115]

---

[110] *Id.* at 43.

[111] *Id.* at 43-44.

[112] *Id.* at 45.

[113] *Id.* at 51.

[114] *Id.* at 40.

[115] On the pre-Katzian themes present in *Kyllo*, see Thomas K. Clancy, *Coping with Technological Change:* Kyllo *and the Proper Analytical Structure to Measure the Scope of Fourth Amendment Rights*, 72 MISS. L.J. 525, 555 (2002) (stating that the "Court's language is remarkable for its reliance on themes developed by the Court when property analysis was the applicable test: the common law; constitutionally protected areas; analogy to physical intrusions; and reliance on what was protected at the time of

Justice Scalia began by noting that the *Katz* approach "has often been criticized as circular" and hence as "subjective and unpredictable,"[116] a criticism that Justice Scalia himself had endorsed in earlier cases.[117] Justice Scalia thus recognized that the purported virtue of the Katzian inquiry, its flexibility, is also its central vice.

Justice Scalia acknowledged that *Katz* may be difficult to refine in some contexts but, importantly, not in that of the home—the context at issue in *Kyllo*—precisely because of the home's common-law historical context of established protections.[118] Justice Scalia here concludes that *Katz* may be applied to the issues raised in *Kyllo* without the approach's characteristic difficulties only because the privacy-in-the-home context of the case allows the Court to return to the common law for guidance. The Court thus rested its application of *Katz* on an analysis of the historical materials which are the foundation of the "protected interest" view rejected by *Katz*. In light of this historical context, Justice Scalia advanced an analysis centering on two basic substantive questions: (i) the nature of the home as a constitutionally protected area under the historically-established principles of the common law and (ii) whether an actual physical intrusion is required to compromise the security of the home triggering the protections of the Fourth Amendment.[119] These questions, which the Court asked in substance, are the same as those presented by the traditional "protected interest" view and expressly condemned by the Court in *Katz*.[120]

On this first point, Justice Scalia recognized that the home is a constitutionally protected area of the highest order. The Fourth Amendment, Justice Scalia acknowledged, recognizes the

---

the framing"); Cloud, *supra* note 71, at 46 (stating that the "core [of the Court's analysis in *Kyllo*] appears to be the functional equivalent of the long forgotten property-based analysis" of Justices in the pre-*Katz* era such as Justice Butler in his *Olmstead* dissent).

[116] *Kyllo*, 533 U.S. at 34.

[117] Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring).

[118] *Kyllo*, 533 U.S. at 34-35 (stating that with the home "there is a ready criterion, with deep roots in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*" (emphasis in original)).

[119] *Id.* at 34-35.

[120] *See* discussion *supra* Part II.A.

traditional "sanctity of the home"[121] and "draws 'a firm line at the entrance to the house,'"[122] so that the "entire [home] area is held safe from prying government eyes" because "all details" in the home are "intimate details" worthy of protection.[123] On the second point, Justice Scalia reasoned that to "assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted," a warrant is presumptively required when police "obtain[ ] by sense-enhancing technology any information . . . that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area.'"[124] The Court thus concluded that police must have a warrant to use a thermal imager.

Of special interest here is Justice Scalia's quotation of language from the Court's decision in *Silverman*—a "physical intrusion into a constitutionally protected area."[125] This is the principal case and almost the very language on which the petitioner in *Katz* relied in crafting the questions presented to the Court, questions which the Court in turn rejected as a "misleading" formulation of the legal issues.[126] Justice Scalia's substantive analysis is also in line with dissenting Justices in the pre-*Katz* *Olmstead* decision, who applied a "protected interest" analysis grounded in the common law in a "liberal" fashion to protect against actual trespasses and other "evils" that are "like and equivalent" to trespasses.[127] In sum, the Court's opinion in *Kyllo* turns on a substantive analysis of the same questions—and in virtually the same language drawn from the pre-*Katz* *Silverman* decision—rejected by the Court as "misleading" inquiries in *Katz*.

---

[121] *Kyllo*, 533 U.S. at 28. "'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" *Id.* at 31 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

[122] *Id.* at 40 (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

[123] *Id.* at 37.

[124] *Id.* at 34 (quoting *Silverman*, 365 U.S. at 512).

[125] *Id.*

[126] Katz v. United States, 389 U.S. 347, 351 (1967).

[127] Olmstead v. United States, 277 U.S. 438, 487-88 (1928) (Butler, J., dissenting); Cloud, *supra* note 71, at 46.

What the opinions in *Kyllo* demonstrate are the problematic framing effects of the Katzian "reasonable expectation of privacy" test. The *Katz* approach frames the question of the applicability of the Fourth Amendment in terms of a governmental invasion of something as open-ended as a "reasonable expectation of privacy" unmoored from any clear legal foundation in the text of the Fourth Amendment or the traditional principles of the common law. Indeed, the lack of mooring is precisely the point of the Katzian approach, and it thus presents the Justices with an inkblot analysis into which they can read their preferences for privacy—or for crime-control polices and deference to government. This approach makes its very easy to characterize *Kyllo* as a case about governmental observation of "external heat emissions" implicating an "at best trivial" privacy concern[128] rather than a case about police use of a technological substitute for an actual physical invasion of the security of Kyllo's home to determine whether Kyllo was committing a crime within its walls.[129] One should not be surprised when four Justices conclude that Kyllo's expectation of privacy is not only "unreasonable" but even "difficult to take seriously."[130]

Compare this with the traditional "protected interest" approach which the majority in *Kyllo* uses in substance while purporting to apply a Katzian analysis. The "protected interest" frame places its emphasis on the textual recitation of protected interests in the Fourth Amendment—persons, houses, papers, and effects—and that emphasizes the centrality and paramount importance of the protection of homes to the meaning of the Fourth Amendment. The Fourth Amendment was in fact designed to protect only four basic interests expressed in its text—and houses are one of those interests. The common-law background principles reinforce that view substantially because those principles affirm the special importance of homes among the four interests.

The "protected interest" doctrinal formulation therefore positions one to read the Fourth Amendment broadly to protect the home. The remaining question, then, is whether to protect the traditional security in the home against both actual physical invasions and the use of cutting-edge technology as a police substitute for such invasions. A court recognizing the importance of security in the home when it answers the first question should be better primed to answer the second question in a home-protective fashion than it otherwise would be.[131] The "protected interest" view, in short, frames the constitutional issues in a way that promotes protection of the home. One should not be surprised when a Court doctrinally committed to *Katz* must struggle to the substance of the "protective interest" view to arrive at and defend a properly home-protective conclusion.

---

[128] *Kyllo*, 533 U.S. at 45 (Stevens, J., dissenting).

[129] *Id.* at 34-35 (majority opinion).

[130] *Id.* at 43 (Stevens, J., dissenting).

C. *"Papers," Digital Documents, and Rival Frames: A Return to "Protected Interests" Within the "Reasonable Expectation of Privacy" Framework?*

The "protected interest" frame underpinning the substantive analysis in *Kyllo* not only promises surer protection for the home, it could also offer more certain protections in other important areas than the Court's present *Katz*-based doctrines. Consider the crucial questions presented by Fourth Amendment protections for "papers"—and their modern digital equivalents such as computer files and e-mail. Suppose that one allows a third party broad access to one's personal papers—such as a diary, letters, or business records—and police in turn obtain the papers from the third party. What implications does this chain of events have for one's Fourth Amendment rights? Do the protections of the Fourth Amendment remain firm or do they falter?

On the "protected interest" view, one would retain one's right to security in the papers against governmental intrusion. The essence of the traditional security in protected interests, grounded in the law of property, is the right to exclude—which, of course, includes the right to selectively include some individuals while excluding others.[132] On this view, one has a right to allow some actors access to one's home or papers while still excluding others—such as the police.[133] It would thus invade the core of the protected interest for the government to obtain papers through a third party and search through them—without the owner's permission.

---

[131] For a notable split on the question of extending protection for the home to functional equivalents of traditional searches, see the majority and dissenting opinions in *Olmstead*, 277 U.S. at 438.

This basic analysis is further reinforced by landmark precedents. The Court held in *Boyd* under the "protected interest" view that simple government compulsion of the production of one's papers implicates the Fourth Amendment because of the invasion of the property interest in the papers.[134] Obviously, the government's use of a third party to achieve the very same end constituting the very same invasion of the property interest in the papers would implicate the amendment equally.[135] As a result, a Court following the "protected interest" view would not approve of a governmental seizure and search of papers simply because the government had employed the stratagem of obtaining the papers through a third party who did not in fact have the owner's authorization to transfer them to police. At a minimum, some additional justification for the search would be required.[136]

---

[132] *See* Clancy, *supra* note 52, at 344-66.

[133] *See id.*

[134] Boyd v. United States 116 U.S. 616, 635 (1886) (stating that the government's strategy of compelling an individual to produce his private papers for government inspection "divested" the government's actions of "many of the aggravating incidents of actual search [for] and seizure" of the papers from the person's home but that the strategy still contained the "substance and essence" and still "effects [the] substantial purpose" of that search and seizure and that "illegitimate and unconstitutional practices get their first footing . . . by [such] silent approaches and slight deviations from legal modes of procedure").

[135] As the *Boyd* Court might put it, asking a third party to turn documents over to the government would limit the "aggravating incidents of an actual search [for] and seizure" of the papers from the person's home, but the strategy still contains the "substance and essence" and still "effects [the] substantial purpose" of that search and seizure. *Id.*

[136] The paper-protective stance of the "protected interest" approach is further reinforced by the traditional mere evidence rule, another facet of the "protected interest" view. The mere evidence rule restricted evidence-gathering searches under the Fourth Amendment and even in its most narrow form protected "papers" from such searches. Thus a traditional "security in protected interest" analysis would actually bar a seizure and search of "papers" for evidence of crime even with a valid warrant. On the mere evidence rule, see *infra* Part IV.

By contrast, under the established Katzian privacy doctrines, granting broad access to one's papers to third parties undermines one's "reasonable expectation of privacy" because one has "knowingly expose[d]"[137] the papers to other persons and could be thought to have "assumed the risk"[138] that those persons will convey the papers and their contents to others—including police.[139] These Katzian points are the basis of the present "third-party doctrine," which holds that there is generally no "reasonable expectation of privacy" in information shared with a third party—even in confidence.[140] The upshot is that today police who obtain papers from a third party may not be viewed as having engaged in a technical "search" under *Katz*. If there is no "search" under *Katz*, no Fourth Amendment protections apply. The "protected interest" approach could thus easily provide more certain protection for papers shared with a third party than the "reasonable expectation of privacy" approach.

Consider the implications of the analysis above for digital documents, which are often shared with others on servers or networks. Even a modestly "liberal" reading of the "protected interest" approach could expand its protections to guard the contemporary equivalents to traditional papers—digital documents such as e-mails and computer files. A "liberal" reading would thus recognize that government access to digital documents through a third party (such as an Internet Service Provider) who is not authorized to grant such access is an invasion of the protected interest in "papers" triggering the protections of the Fourth Amendment. Thus, a government request or demand for digital documents from a third party such as an ISP could not circumvent an individual's protections under the Fourth

---

[137] Katz v. United States, 389 U.S. 347, 351, 360 (1967).

[138] Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding on "assumption of the risk" grounds that there is no "reasonable expectation of privacy" in a conversation with a "false friend" who is cooperating with police to transit the conversation); *cf.* United States v. White, 401 U.S. 745 (1971).

[139] United States v. Miller, 425 U.S. 435, 443 (1976) (stating that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed").

[140] *Id.* at 442.

Amendment. A warrant, consent, or similar justification would still be required to examine the documents.

By contrast, under the Katzian third-party doctrine, the emphasis placed on "knowing exposure" to others and "assumption of the risk" renders digital documents shared with third parties potentially vulnerable to a governmental invasion.[141] Protection under the Katzian framework is uncertain—consistent with the open-ended nature of the Court's "reasonable expectation of privacy" doctrine. While courts applying a broad Katzian framework could ultimately take a protective stance on digital communications under the Fourth Amendment,[142] they will do so by retreating from the full implications of the Court's Katzian third-party doctrine[143] and by returning to the substance of an analysis which emphasizes the importance of the traditional protected interest in "papers"[144]—just as the Court in *Kyllo* found

---

[141] *See, e.g.*, Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1211 (2004) (stating that in light of the Court's third-party doctrine "it remains unclear today whether files held by ISPs on behalf of their users can retain a Fourth Amendment 'reasonable expectation of privacy'").

[142] *See* United States v. Warshak, 631 F.3d 266, 284-89 (6th Cir. 2010) (recognizing a "reasonable expectation of privacy" in e-mail on the facts of the case but holding that the "reasonableness" of the expectation depends in part on the nature of the "subscriber agreement" and the degree to which a commercial ISP intends to monitor e-mail accounts).

[143] *Id.* at 288 (noting the obvious tension between its "reasonable expectation analysis" finding Fourth Amendment protections for e-mail with third-party access and the Supreme Court's third-party doctrine and "assumption of the risk" analysis in *Miller*).

[144] *Cf. id.* at 284 (observing that the "explosion of Internet-based communication" means that "[p]eople are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away" so that the "conglomeration of stored messages that comprises an email account . . . provides an account of its owner's life" into which "government agents" can "peer deeply" into an individual's "activities"). Compare the view in *Warshak* concerning the importance of the individual protected interest in e-mail with Justice Douglas's defense of the protected-interest based mere evidence rule in *Warden v. Hayden*, which emphasizes the importance of both the right to exclude and selectively include others with respect to one's "secrets":

> Those who wrote the Bill of Rights believed that every individual needs both to communicate with others and to keep his affairs to himself. That dual aspect of privacy means that the individual should have the freedom to select for himself the time and circumstances when he will share his secrets with

itself emphasizing the importance of the traditional protected interest in "houses." In sum, the protection of digital documents shared with others is substantially less certain today under the Warren Court's nebulous "reasonable expectation of privacy" approach than it would have been under a "liberal" construction of the traditional "protected interest" approach.

Significantly, the emphasis of each frame tends to shape the outcome here—paralleling the effect of the frames in *Kyllo* for privacy in the home. The "protected interest" analysis places greater emphasis on what interests the Fourth Amendment specifically protects in the constitutional text—here, "papers" in both their original physical and contemporary electronic forms. That emphasis tends to encourage protection by reaffirming the importance of the basic interest at stake—security in papers—and by encouraging a careful evaluation of the underlying reasons for that specific Fourth Amendment protection.[145] That tendency toward protection is further reinforced by the common-law foundation of those interests, which can be extremely protective when "liberally" construed.[146]

The "reasonable expectations of privacy" approach places its central emphasis on the free-floating concept of privacy—with results that are both less predictable and potentially less protective. The result in this context has been a doctrinal focus on the degree to which one has diluted one's "privacy" in papers or digital documents by sharing the documents with other persons who in turn may share them with still other persons—including police. A shift in focus toward "protected interests" and away from "reasonable expectations of privacy" could reduce the potentially negative doctrinal implications of common third-party access to

---

> others and decide the extent of that sharing. This is his prerogative not the States'. The Framers, who were as knowledgeable as we, knew what police surveillance meant and how the practice of rummaging through one's personal effects could destroy freedom.

Warden v. Hayden 387 U.S. 294, 323-24 (1967) (Douglas, J., dissenting). On the demise of the mere evidence rule, see *infra* Part IV.

[145] *See supra* note 144.

[146] The traditional "protected interest" view grounded in property rights both rejects an "assumption of the risk" approach and would have absolutely protected papers from evidence-gathering searches. *See* discussion *supra* Part II.C.

digital documents and offer potentially greater protections for the electronic "papers" which play an increasingly important role in contemporary life.

No radical break with existing doctrine would be required to begin moving down the "protected interest" path to greater protection in this area or in other areas under the Fourth Amendment. *Kyllo* points to a practical way to promote the "protected interest" view to reinvigorate Fourth Amendment rights without overturning established precedents.[147] As it did in *Kyllo*, the Court could slowly reorient the Warren Court's broad "reasonable expectation of privacy" frame back towards a traditional concern for the protection of Fourth Amendment interests specifically enumerated in the text—as "liberally" construed in light of their common-law origins. A cautious doctrinal reorientation rather than a sharp break with precedent is the most prudent path to reform. This Article will discuss Fourth Amendment reform in more detail in Part III.

III. FROM "SECURITY" IN PROTECTED INTERESTS TO THE "REASONABLENESS" OF POLICE CONDUCT

A. Rival Frames: "Security" Versus "Reasonableness"

Doctrinal constructions determining the applicability of the Fourth Amendment must be followed by another set of doctrines that determine when the protections of the amendment are satisfied. If the protections of the Fourth Amendment apply, which governmental actions comply with the amendment and which do not comply? The text of the Fourth Amendment guarantees "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."[148] Another fundamental division in doctrinal construction is whether to emphasize the text of "security" (in persons, houses, papers, or effects)[149] or the textual prohibition of "unreasonable" searches and seizures.[150]

---

[147] *See* Cloud, *supra* note 100, at 73 n.144.

[148] U.S. CONST. amend. IV.

Should one privilege the concept of "security" and subordinate the concept of Fourth Amendment "unreasonableness" by defining the latter largely or wholly in terms of "security" in protected interests? On this view, searches that unjustifiably compromise "security" in "persons, houses, papers, and effects," properly understood, are "unreasonable" for that reason. Or should one privilege the concept of "unreasonableness" and subordinate the concept of Fourth Amendment "security" by defining "security" largely or wholly in terms of freedom from "unreasonable" searches? On this view, it is only from "unreasonable" searches that one has any right to be secure. Does one want a doctrinal analysis formulated principally as a positive statement of the interests of the people worthy of special protection (i.e., security in protected interests) or principally as a negative statement of the police conduct one wishes specially to prohibit (unreasonable searches)? What word and concept—"security" or "unreasonableness"—should drive the doctrinal formulation? This is a basic question of doctrinal framing.

One should also note here the immediate framing effect of our last doctrinal crossroads—whether, when thinking about the initial applicability of the Fourth Amendment, to emphasize the text of "persons, houses, papers, and effects" or the textual reference to "searches" doctrinally defined in terms of "reasonable expectations of privacy." That choice of frame has implications for the next choice of frame given the text of the Fourth Amendment. The word "secure" in the text is closely associated with the phrase "persons, houses, papers, and effects." The guarantee of "security" is extended to four enumerated interests: "the right of the people to be secure in their persons, houses, papers, and effects." Therefore, the "protected interest" view emphasizing "persons, houses, papers, and effects" will tend to gravitate toward the word

---

[149] On the general concept of Fourth Amendment "security" in "protected interests," see Clancy, *supra* note 52.

[150] On the general concept of Fourth Amendment "reasonableness," see Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977.

"secure" and the concept of "security" in formulating a doctrine on the question of Fourth Amendment standards. On the other hand, the word "unreasonable" in the Fourth Amendment modifies the word "searches," and thus the Katzian view emphasizing the invasion of a "reasonable expectation of privacy" as a Fourth Amendment "search" will tend to gravitate toward the word and concept of "(un)reasonableness" in formulating a doctrine. In sum, *Katz*'s doctrinal reformulation of the focus of the application of Fourth Amendment law has a major framing effect on the doctrinal question of when the Fourth Amendment is satisfied, one that promotes a frame focused on "(un)reasonableness."

Consider another hypothetical drawn from the area of consent searches—one based on the facts of *Illinois v. Rodriguez*.[151] Police search a home with the consent of someone who claims to live in the home and to have authority to consent to a search but who in fact is a former resident of the home without authority to consent. The police form a reasonable belief in the person's authority to consent based upon evidence that the person lives in the house. The police search clearly triggers the protections of the Fourth Amendment because there is a "search" under *Katz* (and would also trigger the protections of the Fourth Amendment under the "protected interest" view because there is a physical invasion of a "house"), but the question remains: Have those protections been complied with? Should our doctrinal analysis emphasize "security" in the person's house or the "reasonableness" of the police conduct? When one frames the question, will one ask principally whether the individual's house was properly "secure" or whether the police engaged in an "unreasonable" search?

The "security" perspective encourages one to approach the doctrinal question from the perspective of what the Fourth Amendment was meant to protect—here the individual's security in the home—and to adopt what amounts to a resident-oriented perspective asking whether the individual's home was properly secure or unjustifiably compromised. The "reasonableness" perspective encourages one to approach the doctrinal question from the perspective of what the Fourth Amendment was meant to prohibit—unreasonable searches—and might tend to promote a police-oriented perspective (asking whether the officers acted reasonably in light of what they knew or should have known).

---

[151] Illinois v. Rodriguez, 497 U.S. 177 (1990).

These two different ways of framing the issue have the potential to shape intuitions and push answers in different directions—just as the framing of consent search analysis does in other ways (as a Fourth Amendment waiver or a Katzian non-search). The first approach centered on "security" is likely to generate deference toward the interests of residents because the word "security" is paired with the word "house" and thus places analytical emphasis squarely on the individual's security in the home and the importance of its protections under the Fourth Amendment. The second approach centered on "reasonableness" is more likely to generate deference toward police because it places its analytical emphasis on the objective behavior of police and because the stated standard requires that police be merely "reasonable." Indeed, one should not underestimate here the power of the word "reasonable" in this context to facilitate the argument that the Fourth Amendment requires from police "mere" reasonableness in a simple criminal justice policy sense rather than in a traditional Fourth Amendment justificatory sense (e.g., a warrant or actual consent).[152]

While intuitions will no doubt vary, the first approach above seems to offer a more straightforward promise of broad protection. If one asks in this hypothetical situation whether the citizen's home as a constitutionally protected area was properly secure, one will be inclined to focus on the police entry into the home and the absence of a warrant or actual consent as traditional justifications for that entry. One will then tend to ask whether the police had another justification for their search analogous to a warrant or actual consent.[153] The officer's reason for searching in this example—a reasonable mistake about consent—has more of the character of an excuse than a justification for the search and is a far cry from a warrant or actual consent. However, if one asks whether the police officer's search was a reasonable one, one can easily answer in the affirmative—because the police reasonably believed that they had consent.[154]

---

[152] *See* discussion *infra* Part III.B. on the "security-driven" view of "reasonableness."

[153] *Cf.* Gouled v. United States, 255 U.S. 298 (1921) (holding that an entry into a home without a warrant and without consent by force, coercion, or stealth are all equally without justification and therefore equally violative of the Fourth Amendment).

These divergent framing effects may be most important when judicial actors who must answer the question have strong crime-control policy inclinations. The "security" frame tends to center the issue on the individual interest invaded by police and the need for a compelling justification for such action and may act to constrain crime-fighting policy inclinations to some substantial degree, while the "reasonableness" frame tends to center the issue on an appraisal of police under a standard which invites an open-ended consideration of policy such as the suppression of crime. Significantly, the Court's actual conclusion in *Illinois v. Rodriguez* is the most straightforward product of the "reasonableness" frame used by the Court today: if police "reasonably" believe someone has authority to consent and has in fact consented, the search is "reasonable."[155] The dissent in *Rodriguez*, written by Justice Marshall, had to fight the uphill battle of explaining why a search based upon a "reasonable" mistake about consent would still be "unreasonable" as a matter of Fourth Amendment law.[156] It would have been much easier for Justice Marshall's view to prevail if the doctrinal frame had more effectively emphasized the invasion of security in the home and the need for a strong justification for such action.

B. The "Security" Era and the Warren Court's Transition to the "Reasonableness" Era

As *Rodriguez* illustrates, the Court's analysis today is centered on "reasonableness," and "security" is seldom seriously considered as an independent concept. While the distinction between the "security" and "reasonableness" doctrinal frames is not quite as sharp as a matter of constitutional history as the distinction between "protected interests" and "reasonable expectations of privacy," the distinction still captures an essential difference between the Court's conception of the Fourth Amendment in the pre- and post-Warren Court eras. The Fourth Amendment jurisprudence of earlier days did not always emphasize the precise terminology of "security" over that of "reasonableness,"[157] but it did regularly define "reasonableness" in the Fourth Amendment in light of the common-law background of property rights which form the foundation of the traditional view of "security" in protected interests.[158] This "security" focus routinely led the Court to emphasize both the Fourth Amendment's substantive protections derived from common-law property rights[159] and its procedural protections for "security" in protected interests associated with doctrines such as the warrant preference.[160] The result was a protective set of substantive and procedural requirements.

---

[154] *Rodriguez*, 497 U.S. at 185-87.

[155] *Id.*

[156] *Id.* at 189. (Marshall, J., dissenting).

It was *Boyd v. United States*, the landmark case of the 1880s, which first expressly adopted this common-law approach to the Fourth Amendment equating "reasonableness" in part with respect for the property rights implicated by the security of the enumerated interests in the Fourth Amendment.[161] This security-driven view of "reasonableness" is on display in the evolution of the primary substantive protection for security in protected interests, the mere evidence rule prohibiting evidence-gathering searches, as will be discussed in detail in Part IV of this Article.[162] The security-oriented view of "reasonableness" is also embodied in early cases endorsing the primary procedural protection for security, the warrant preference.[163] The Court viewed this mechanism as the vehicle "the framers of the Fourth Amendment" embraced to "provide the necessary security against unreasonable intrusions upon the private lives of individuals."[164] Notably, the traditional security-driven view of the Fourth Amendment was substantially eroded by the Warren Court in the 1960s as part of its criminal procedure revolution.[165] That Court—in pivotal cases such as *Schmerber v. California*,[166] *Warden v. Hayden*,[167] and *Terry v. Ohio*[168]—adopted something closer to a contemporary view of "reasonableness" that generally equates that standard with a flexible and policy-oriented evaluation of police conduct not tied to the formal enumeration of protected interests in the Fourth Amendment or their traditional common-law context.[169]

---

[157] *Boyd v. United States* may have been first case to treat "(un)reasonableness" as an independent standard apart from the standards for warrants in the second clause of the Fourth Amendment. Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 728 n.514 (1999).

[158] *See* Hoffa v. United States, 385 U.S. 293, 301 (1966) ("What the Fourth Amendment protects is the security a man relies upon when he places himself or his property within a constitutionally protected area, be it his home or his office, his hotel room or his automobile."); Clancy, *supra* note 150, at 991-92; *cf.* Illinois v. Andreas, 463 U.S. 765, 776 n.4 (1983) (Brennan, J., dissenting) (stating that "[b]efore *Katz*, this Court may have focused too much on the 'security' aspect of the right of privacy, while giving short shrift to its 'secrecy' aspect").

[159] *See* Gouled v. United States, 255 U.S. 298 (1921); Clancy, *supra* note 150, at 991-92.

[160] *See* Weeks v. United States, 232 U.S. 383, 393 (1914) (stating that police "could only have invaded the house of the accused when armed with a warrant issued as required by the Constitution").

[161] Boyd v. United States, 116 U.S. 616 (1886).

Not surprisingly, a broad range of cases from the earlier era give a decided emphasis to "security" as a word and concept driving the definition of "reasonableness."[170] For instance, in *Gouled v. United States* in 1921, the Court held that entry into a home without a warrant by stealth was no better than entry without a warrant by force or coercion.[171] Why? Because, the Court said "[t]he *security* . . . of the home . . . would be as much invaded and . . . as much against [the] will [of the owner] in the one case as in the other, and it must therefore be regarded as equally in violation of his constitutional rights."[172] The Court in *Gouled* placed a special emphasis on the "security" of the "protected interest" and then defined "unreasonableness" largely in light of that emphasis. One can easily apply *Gouled*'s traditional "security" in "protected interests" thought to our consent search hypothetical above based upon *Illinois v. Rodriguez*: When police enter a home without a warrant—whether by force, coercion, stealth, or *simple mistake*—the security of the home is equally invaded against the will of the owner, so each must be regarded equally as a violation of constitutional rights. Notably, the pre-Warren era *Gouled* Court would likely have extended more protection to the resident in "apparent authority" circumstances than the post-Warren era *Rodriguez* Court did almost seventy years after *Gouled*.

---

[162] *See infra* Part IV.

[163] Trupiano v. United States, 334 U.S. 699, 705 (1948).

[164] *Id.*

[165] *See* Clancy, *supra* note 150, at 992; *infra* Part III.

[166] 384 U.S. 757 (1966).

[167] 387 U.S. 294 (1967).

[168] 392 U.S. 1 (1968).

[169] *See* Clancy, *supra* note 150, at 1005-11.

[170] *See, e.g.*, Trupiano v. United States, 334 U.S. 699, 705 (1948).

[171] Gouled v. United States, 255 U.S. 298 (1921).

[172] *Id.* at 305-06 (emphasis added).

Another illustrative case from this era of "security-driven" conceptions of "reasonableness" is *Johnson v. United States*.[173] In *Johnson*, police searched a hotel room without a warrant after detecting the scent of burning opium in a hallway.[174] The Court stated that the "right of officers to thrust themselves into a home is . . . a grave concern, not only to the individual but to a society which chooses to dwell in *reasonable security* and freedom from surveillance."[175] The Court therefore endorsed a strong "warrant preference" so that probable cause determinations will be made by a "neutral and detached magistrate" rather than by potentially overzealous officers "engaged in the often competitive enterprise of ferreting out crime."[176]

The Court in *Johnson* acknowledged that "[t]here are exceptional circumstances in which . . . it may be contended that a magistrate's warrant for search may be dispensed with" but stated that "[n]o reason is offered for not obtaining a search warrant" in this case except for "inconvenience" and "some slight delay."[177] *Johnson* thus stands for the view that the people's "reasonable security" in their "persons, houses, papers, and effects" requires that police act under the authority of a warrant except in "exceptional circumstances." It is unlikely that the *Johnson* Court would have concluded that a "reasonable mistake" about consent is such an "exceptional circumstance."

---

[173] 333 U.S. 10 (1948).

[174] *Id.* at 12.

[175] *Id.* at 14 (emphasis added).

[176] *Id.*

[177] *Id.* at 14-15.

The abandonment of the "protected interest" view—a view grounded in the specific enumeration of interests in the Fourth Amendment, in the common law, and in pre-Warren Court precedents—fatally undercut the traditional security approach on display in *Gouled* and *Johnson*. The Warren Court's move to newer approaches to the Fourth Amendment emphasizing interpretive flexibility, the ephemeral promise of greater protections for privacy, and the textual reference to "searches" all ensured that an analysis of "reasonableness" as an open-ended policy-oriented standard would predominate and be subject eventually to security-restrictive crime-control interpretations as the political orientation of the Court as a whole moved to the right. The full fruit of the new approach to Fourth Amendment "reasonableness" is on display in *Rodriguez*, as discussed above, and can also be seen in cases such as *Michigan v. Summers*[178] and *Michigan Department of State Police v. Sitz*.[179]

Consider the last two cases. *Michigan v. Summers* involved a detention without probable cause of an occupant of premises subject to search under a search warrant.[180] The Court upheld the detention as a "reasonable" seizure despite the absence of probable cause to arrest by "balancing" the intrusion on the interests of the individual against law enforcement interests.[181] The Court found the intrusion on individual interests to be minimal since few persons would wish to leave during a police search of their homes while the law enforcement interests were pressing given the suspicion that attaches to someone whose home is subject to search and the concerns about the flight of suspects and risk of harm to the officers.[182] *Sitz* involved the question of seizures at a sobriety checkpoint.[183] The Court concluded that the seizure at the sobriety checkpoint was "reasonable" under the Fourth Amendment despite the absence of any individualized suspicion for the seizure by simply balancing the effectiveness of the checkpoint in serving the state interest in safe roadways against the intrusion on the individuals seized.[184] The Court also observed in *Sitz* that "the choice among . . . reasonable alternatives remains with the governmental officials" given their "unique understanding of" and unique "responsibility" for "limited public resources."[185]

---

[178] 452 U.S. 692 (1981).

[179] 496 U.S. 444 (1990).

[180] 452 U.S. 692 (1981).

[181] *Id.* at 699-704.

[182] *Id.*

[183] 496 U.S. at 444.

By *Rodriguez*, *Summers*, and *Sitz*, Fourth Amendment "reasonableness" is a flexible standard, and its flexibility is employed by a Court with a strong interest in facilitating the control of crime and deferring to local authorities. In these decisions, police behavior which is viewed as "reasonable" in a crime-control policy sense is also viewed as "reasonable" under the Fourth Amendment. Dissenting Justices in these cases invoked the importance of traditional justifications for government searches and seizures—the warrant preference in *Rodriguez*,[186] the probable cause standard in *Summers*,[187] and individualized suspicion in *Sitz*[188]—but the invocation of such traditional justifications as a constraint on judicial policy evaluation under the "reasonableness" standard had already been seriously undermined by the Warren Court's own policy-oriented rejection of similar protective doctrines grounded in Fourth Amendment tradition.[189] One traditional protection discarded by the Warren Court under a flexible "reasonableness" approach to the Fourth Amendment was the mere evidence rule.[190] In Part IV, this Article will discuss that issue and its broader consequences for Fourth Amendment "reasonableness."

---

[184] *Id.* at 450.

[185] *Id.* at 453-54.

[186] Illinois v. Rodriguez, 497 U.S. 177, 189 (1990) (Marshall, J., dissenting).

[187] 452 U.S. at 706 (Stewart, J., dissenting).

[188] 496 U.S. at 456 (Brennan, J., dissenting). Justice Thomas has also expressed interest in reconsidering *Sitz*, stating that it is "rather doubt[ful] that the Framers of the Fourth Amendment would have considered 'reasonable' a program of indiscriminate stops of individuals not suspected of wrongdoing." City of Indianapolis v. Edmond, 531 U.S. 32, 56 (2000) (Thomas, J., dissenting).

[189] *See* Terry v. Ohio, 392 U.S. 1 (1968); Warden v. Hayden, 387 U.S. 294 (1967); Schmerber v. California, 384 U.S. 757 (1966).

[190] *Warden*, 387 U.S. at 294.

C. The Continuing Relevance of the "Security" Frame in the Court's Decisions Today

Significantly, the "security" frame is still relevant to the Court's Fourth Amendment analysis, and its undervalued potential to promote a reinvigorated protection of Fourth Amendment rights can be seen in the opinions in the recent case of *Kentucky v. King*.[191] That case concerned the issue of police-created exigencies and warrantless entries into the home.[192] Justice Alito, writing for the Court in *King*, concluded that warrantless searches of homes are generally justified by police-created exigent circumstances except when the police create the exigency "unreasonably" by "engaging or threatening to engage in conduct that violates the Fourth Amendment."[193]

Justice Alito's opinion is a straightforward application of the dominant "reasonableness" frame with its current crime-control orientation: police act "reasonably" as a general matter when their warrantless search is the product of an exigency unless they have created the exigency "unreasonably" by violating or threatening to violate the Fourth Amendment. No special concern for security in the home is evident in the opinion beyond a pro forma recognition of the original policy basis for the warrant preference.[194] The free-floating "reasonableness" of the police conduct with a focus on efficient control of crime is almost the sole focus.[195]

Justice Ginsburg, the lone dissenter in *King*, countered the majority's "reasonableness" analysis by building much of her analysis of the issue around the rival concept of "security" as supported by text, tradition, and precedent from the "security" era.[196] She contended that police who pass on the opportunity to obtain a search warrant and act instead to create an exigency cannot invoke the exigency as a basis for a warrantless entry into the home.[197] In framing her argument, Justice Ginsburg reoriented the "reasonableness" frame toward "security" by specially emphasizing the security language in the Fourth Amendment: "The Fourth Amendment guarantees to the people '[t]he right . . . to be secure in their . . . houses . . . against unreasonable searches and seizures.'"[198]

---

[191] 131 S. Ct. 1849 (2011).

[192] *Id.*

[193] *Id.* at 1858.

[194] *Id.* at 1856.

[195] *Id.* at 1860-61 (recounting "legitimate law enforcement strategies" that would be "unjustifiably" restricted by additional limits on the use of police-created exigencies to justify warrantless entries into and searches of the home).

[196] *Id.* at 1864-66 (Ginsburg, J., dissenting).

Justice Ginsburg further grounded her analysis in the security-driven common-law traditions dating back "centuries" that extend special protections to the home, a point of argument which functions as a "security" bulwark against the majority's "reasonableness" crime-control impulse.[199] Further, she drew on *Johnson v. United States* from the "security" era to define "reasonableness" in terms of a strict warrant preference providing "reasonable security and freedom from surveillance" in the home.[200] Finally, Justice Ginsburg pointed to the serious consequences of the Court's free-floating "reasonableness" analysis in *King* for Fourth Amendment "security" in the home—asking rhetorically: "How 'secure' do our homes remain if police, armed with no warrant, can pound on doors at will and, on hearing sounds indicative of things moving, forcibly enter and search for evidence of unlawful activity?"[201]

Kentucky v. King, in sum, shows the importance of the rival frames for Fourth Amendment rights and the relevance today of their conflicting approaches. The Justices deploying the dominant free-floating "reasonableness" approach predictably reached a conclusion favoring law enforcement over protecting the security of the home. Justice Ginsburg, defending a home-protective conclusion, found herself reorienting the "reasonableness" doctrine toward the traditional "security" frame in order to craft the most persuasive legal argument for her position. The opinions in *King* demonstrate both the need for a doctrinal reform of Fourth Amendment "reasonableness" and point to a particular path paralleling that in *Kyllo*: gradually rebuilding traditional "security" concerns back into the substance of the Warren Court's open-ended "reasonableness" frame. This Article will discuss the future of Fourth Amendment reform in more detail in Part V.

---

[197] *Id.* at 1864.

[198] *Id.* (ellipses in original).

[199] *Id.* at 1865.

[200] *Id.* at 1866 (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)). Justice Ginsburg also points to powerful home "security" language from *Silverman*, language also quoted by the Court in *Kyllo* as part of its return to a more traditional emphasis: "At [the Fourth Amendment's] very core stands the right of a man to retreat to his own home and there be free from unreasonable governmental intrusion." *Id.* at 1865 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

[201] *Id.* at 1865.

IV. RE-ANCHORING THE FOURTH AMENDMENT: FROM A SUBSTANTIVE BAN ON EVIDENCE-GATHERING SEARCHES TO FACILITATING THE CONTROL OF CRIME

A. The Mere Evidence Rule

In *Warden v. Hayden*, the Warren Court discarded the traditional mere evidence rule barring evidence-gathering searches,[202] and the Court's pivotal decision in that case was an essential part of its revolution in criminal procedure. In *Hayden*, the Court confronted a basic doctrinal question: Does the Fourth Amendment allow police to search a home for "mere evidence" of crime—as opposed to searching for contraband, fruits of crime, or criminal instrumentalities—if the officers have a procedural justification for the search such as a valid search warrant or an exigency?[203] Under the broad view of the mere evidence rule then in force, evidence searches were impermissible under the Fourth Amendment. The Court in *Hayden* repudiated the mere evidence rule in toto and approved evidence searches generally. The Court's resolution of this question in *Hayden* stands in stark contrast to the traditional "security in protected interest" view of the matter.

The traditional view reflected in the Court's longstanding precedents held that police may not search for "mere evidence" of crime, that such a search is substantively barred by the Fourth Amendment even with a valid warrant or similar justification.[204] This traditional bar, known as the mere evidence rule, had a lengthy legal pedigree dating back in one form or another to the prohibition of "paper searches" for evidence in the English common law.[205] The new view, expressed in *Hayden* as part of the Warren Court's shift to an innovative free-floating "reasonableness" analysis of the Fourth Amendment's requirements, [206] holds that police may search for mere evidence of crime if they possess a valid warrant or similar justification.[207] The Warren Court's view in *Hayden* is that Fourth Amendment "reasonableness" requires no more than adherence to such procedural protections.[208]

---

[202] 387 U.S. 294 (1967).

[203] *Id.*

[204] Gouled v. United States, 255 U.S. 298 (1921).

The traditional mere evidence rule will strike many readers today as an unsound doctrine—an "irrational" obstacle to effective law enforcement—which the Court was right to abandon.[209] Serious arguments can certainly be made for that position,[210] and it is ultimately impossible to determine to what extent that view today has been influenced by the anchoring effects of the Court's present Fourth Amendment doctrines. On the other hand, distinguished jurists have defended the mere evidence rule as an essential component of Fourth Amendment liberty[211]—a view which itself is no doubt partly the product of an earlier set of anchors.[212] Moreover, if the mere evidence rule seems problematic in a broader form which bars all evidence-gathering searches, it is certainly much less problematic in its narrower original form which bars evidence-gathering searches only of an individual's "papers," a limited "mere evidence" restriction which would allow other forms of evidence-gathering searches.[213] Additionally, the

---

[205] *See Hayden*, 387 U.S. at 313 (Douglas, J., dissenting).

[206] Notably, the Court in *Schmerber* first broke with mere evidence rule *sub silentio* a year before *Hayden* by upholding a "search" of an individual's blood for evidence of driving under the influence of an intoxicant. *See* Schmerber v. California, 384 U.S. 757 (1966).

[207] *Hayden*, 387 U.S. at 310-11 (Fortas, J., concurring).

[208] *Id.* at 309-10.

[209] *Id.* at 302, 309-10.

[210] This view is expressed, most obviously, in *Hayden* itself. *See id.*

[211] *See id.* at 312-25 (Douglas, J., dissenting).

[212] Justice Douglas, dissenting in *Hayden*, defends the mere evidence rule, and his defense was likely "anchored" by both Supreme Court precedents and the traditions of the common law. *See id.*

[213] The mere evidence rule originated in "paper" search cases such as *Entick v. Carrington* and *Boyd*, and the principal concern motivating the rule in these cases can be viewed as the extreme invasiveness of the "paper" search on individual interests,

Court's rejection of any clearly established individual right under the Constitution—grounded in history, tradition, and precedent—is surely cause for real concern.

Even so, this Article is ultimately less concerned with the (de)merits of the mere evidence in isolation—whether in broad or narrow form—than it is with the broader consequences of the Court's peremptory abandonment of the rule for the development of other Fourth Amendment doctrines. In particular, this Article advances the view that the Warren Court's wholesale rejection of the mere evidence rule helped to legitimate a revisionist crime-control approach to Fourth Amendment "reasonableness" and eliminated a powerful doctrinal anchor in favor of a rights-protective understanding of the Fourth Amendment. It is to the foundation of these questions that this Article now turns.

B. The Rival Frames and Evidence-Gathering Searches

One can begin to explore the consequences of the Court's decision in *Hayden* by asking why the rival frames associated with the Fourth Amendment embraced different views of the legitimacy of evidence-gathering searches. The traditional "protected interest" view is rooted in the text of "security" in "persons, houses, papers, and effects" and in the background principles of the common law of property that provide the principal historical context of that text.[214] The "protected interest" view recognized the mere evidence rule first and foremost because that rule is rooted in the Fourth Amendment's historical context in the common law of property.[215]

On this basis, courts recognized a distinction grounded in property interests between a governmental search for items

---

though broader language invoking property rights and justifying a broader form of the rule appears in both cases. A powerful argument can be made that the Court, prior to *Hayden*, had interpreted the mere evidence rule much too broadly to apply to all evidence-gathering searches and that the rule in its original narrow form confined to the "paper" search context of *Entick* and *Boyd* is quite defensible as a matter of Fourth and Fifth Amendment law and public policy. For a discussion of these points, see Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 593-98 (1996).

[214] *See* Clancy, *supra* note 52, at 309-27; Clancy, *supra* note 150, at 991-92.

[215] *See* Clancy, *supra* note 52, at 309-27.

subject to seizure without a trespass on the owner's property rights—such as stolen goods which the government is recovering for the lawful owner or contraband goods which cannot be lawfully owned by anyone—and items not subject to seizure without a trespass because the items are lawfully owned even though they also happen to be evidence of crime.[216] On this view, the government could search for and seize stolen goods, contraband, and criminal instrumentalities because such searches are consistent with respect for individual property rights, but government could not search for and seize "mere evidence" of crime constituting lawfully owned property which the government has no right to take from its legitimate owner.

The legal pedigree of the mere evidence rule is quite strong. Lord Camden in the celebrated English case of *Entick v. Carrington* in 1765 condemned evidence searches of private papers,[217] and this decision arguably formed a part of the framers' understanding of the common-law background of the Fourth Amendment.[218] In *Entick*, Lord Camden noted that even when the government is investigating crimes such as "murder, rape, [or] robbery" the common law "provide[s] no paper search [for evidence] in [such] cases to help forward the conviction[ ]."[219] Lord Camden explained that the policy for this rule grounded in respect for property rights in papers might be found in either "a consideration that such a power would be more pernicious to the innocent than useful to the public" or perhaps "the gentleness of the law towards criminals."[220]

---

[216] Entick v. Carrington, 19 How. St. Tr. 1029 (1765), 95 Eng. Rep. 807 (K.B. 1765).

[217] *Id.*

[218] *See* Clancy, *supra* note 52, at 309-27. Scholars continue to dispute the influence of *Entick* on the framers and the standing of the mere evidence rule as part of the original understanding of the Fourth Amendment. *See* Roger Roots, *The Originalist Case for the Fourth Amendment Exclusionary Rule*, 45 GONZ. L. REV. 1 (2010) (contending the framers of the Fourth Amendment embraced the mere evidence rule and that *Entick* or similar common-law sources shaped their views on the question); Davies, *supra* note 157, at 727 n.513 (contending that framers did not embrace the mere evidence rule and were likely not influenced by any discussion of the rule in *Entick*).

[219] *Entick*, 19 How. St. Tr. at 1073.

[220] *Id.*

The Supreme Court embraced Lord Camden's view in *Boyd v. United States* in 1887, and the Court stated that "every American statesman, during our revolutionary and formative period as a nation, was undoubtedly familiar with [*Entick* as a] monument of English freedom" and "considered it as the true and ultimate expression of constitutional law."[221] The Court in *Boyd* concluded that *Entick*'s understanding of the common law of search and seizure governed the Fourth Amendment because *Entick*'s "propositions were in the minds of those who framed the fourth amendment to the constitution."[222] In *Gouled v. United States* in 1921, the Court finally expressly formalized the adoption of the mere evidence rule in a decision without a single dissenter.[223] Justice Clarke, citing *Boyd*, stated for the Court that search warrants "may not be used as a means of gaining access to a man's house or office and papers solely for the purpose of making [a] search to secure evidence to be used against him in a criminal or penal proceeding."[224] To search, the government must be looking for items such as stolen goods or contraband.[225] Notably, Congress through this period had never authorized federal magistrates to issue search warrants to seize mere evidence of crime.[226]

The Warren Court's doctrinal revolution eroded the foundations of the mere evidence rule. The Court's new analysis rejected a traditional framework placing an emphasis on the security of protected interests within a common-law property context and instead embraced a new approach placing an emphasis on "reasonableness" inquiries. As part of this transition to these new "reasonableness" doctrines, the Court not surprisingly scrapped the common-law property-based mere evidence rule.[227]

---

[221] 116 U.S. 616, 626-27 (1886).

[222] *Id.*

[223] 255 U.S. 298 (1921).

[224] *Id.* at 309.

[225] *Id.* The Court later expanded the range of items which the government could search for consistent with the mere evidence rule to include criminal instrumentalities broadly defined. *See* Marron v. United States, 275 U.S. 192 (1927).

[226] Warden v. Hayden, 387 U.S. 294 (1967). The Court in *Hayden* notes that "[e]ven in the Espionage Act of 1917, where Congress for the first time granted general authority for the issuance of search warrants, the authority was limited to fruits of crime, instrumentalities, and certain contraband." *Id.* at 308.

Justice Brennan, writing the opinion of the Court in *Hayden*, in fact offered a range of reasons for the Court's sharp break with precedent. Justice Brennan first pointed to the text of the Fourth Amendment and its failure specifically to enumerate the mere evidence rule as a constitutional protection.[228] He also argued that the distinction between mere evidence of crime and stolen goods, contraband, and criminal instrumentalities was "irrational" and did not protect Fourth Amendment privacy interests in any principled fashion.[229] Further, the government has a general interest in "solving crime," Justice Brennan observed, quite apart from the question of whether the items sought by police are contraband or stolen goods.[230] Finally, while not disputing the historical pedigree of the mere evidence rule in the common law and in American cases, Justice Brennan pronounced the rule's grounding in property interests "discredited" by the recent evolution of American law.[231] Newer decisions, Justice Brennan contended, had endorsed a more direct protection of privacy interests through procedural mechanisms such as the warrant requirement and the remedy of the exclusionary rule.[232] In short, despite the mere evidence rule's deep foundations in the common law and in precedent, the Court felt free to discard the entire rule under a flexible interpretation of "reasonableness."

Three of the Court's liberal Justices in *Hayden* would have retained the mere evidence rule at least in part. Justice Fortas, joined by Chief Justice Warren, concurred in the Court's judgment but refused to join the majority's "broad . . . repudiation" of the mere evidence rule.[233] Justice Fortas preferred instead to embrace the creation of an additional exception to the rule tailored for the case at hand involving "hot pursuit" of a suspect and the seizure of

---

[227] *Id.* at 309-10.

[228] *Id.* at 301-02.

[229] *Id.* at 302, 309-10.

[230] *Id.* at 306.

[231] *Id.*

[232] *Id.* at 306-09.

[233] *Id.* at 310 (Fortas, J., concurring).

"identifying clothing worn in the commission of a crime."[234] Justice Fortas, in sum, would have further narrowed the mere evidence rule but not—as he described it—"needlessly destroy[ ], root and branch, a basic part of liberty's heritage."[235]

Justice Douglas dissented—advancing a defense of the mere evidence rule as a fundamental part of the broad protections the Fourth Amendment guarantees to the people.[236] The Fourth Amendment, Justice Douglas recognized, had two deeply-rooted historical zones of protection, a procedural zone embodied in the warrant preference and a substantive zone reflected in the mere evidence rule, and he viewed both zones as protections of vital importance to the rights of the individual.[237] Justice Douglas recounted at length the mere evidence rule's deep roots in English common law and summarized the rule as one:

> [creating] a zone that no police can enter—whether in "hot pursuit" or armed with a meticulously proper warrant—[a crucial point] emphasized by *Boyd* and by *Gouled*. [These cases] have been consistently and continuously approved. I would adhere to them and leave with the individual the choice of opening his private effects (apart from contraband and the like) to the police or keeping their contents a secret and their integrity inviolate. The existence of that choice is the very essence of the right to privacy.[238]

Justice Douglas, in short, would have retained the mere evidence rule as both a historically-established rule and one ultimately essential to the protection of privacy.

The Court in *Hayden* rejected the views of these three Justices, repudiating the mere evidence rule in its entirety. No one can doubt that the demise of the mere evidence rule—for good or ill—fundamentally contracted the Fourth Amendment's guarantee of "security" in "persons, houses, papers, and effects" by eliminating the substantive dimension of that guarantee against government evidence-gathering searches and diverting the protection of Fourth Amendment rights to the procedural dimensions of the guarantee.[239] This was a fundamental shift in Fourth Amendment law, one which narrowed traditional protections and which also eliminated a doctrinal "forward base" that could have been used to build on those protections. This contraction in rights itself is also notable given the Warren Court's reputation for expanding the protections afforded to the individual rights under the Constitution.[240] Its possible implications for other Fourth Amendment doctrines are also quite disturbing.

---

[234] *Id.* at 312.

[235] *Id.*

[236] *Id.* (Douglas, J., dissenting).

[237] *Id.* at 313.

[238] *Id.* at 325 (footnote omitted).

C. Re-Anchoring Fourth Amendment "Reasonableness" in Crime-Control Policies

Not only did the Court dispense entirely with the substantive "zone" of security protected by the mere evidence rule, the discarding of the rule has almost certainly influenced later decisions and had substantial anchoring effects on Fourth Amendment "reasonableness" analyses more generally. As recounted in Parts II and III, the Court has reframed the basic application of the Fourth Amendment from a traditional emphasis on the "security" of "protected interests" to forms of "reasonableness" analysis—both the reasonableness of the expectation of privacy that the government has invaded and the reasonableness of the governmental invasion itself. These reasonableness analyses often produce either free-floating "inkblot" approaches to "reasonableness" (e.g., *Illinois v. Rodriguez*[241]) or a more elaborate "balancing" approach to "reasonableness" which weighs the individual interest against the social interest in crime control (e.g., *Summers*[242] and *Sitz*[243]).

The sweeping rejection of the mere evidence rule was part of this fundamental reframing of the Fourth Amendment around open-ended "reasonableness" tests, and one can easily conceive of

---

[239] *See* Cloud, *supra* note 100, at 55-59.

[240] *See id.*

[241] 497 U.S. 177 (1990).

[242] Michigan v. Summers, 452 U.S. 692 (1981).

[243] Mich. Dept. of State Police v. Sitz, 496 U.S. 444 (1990).

Justice Brennan's opinion for the Court in *Hayden* as a template for later crime-control decisions under the Fourth Amendment, decisions which routinely provoked a dissent from Justice Brennan and the Court's more liberal Justices. The template on display in *Hayden* has the following basic pattern: (1) the Court states that the protection at issue, however strong its historical pedigree, is not specifically enumerated in the text of the first clause of the Fourth Amendment, which prohibits "unreasonable" searches and seizures—without defining "unreasonableness";[244] (2) the Court asserts that a recognition of the protection is not necessary to serve the ultimate policy interests underlying the Fourth Amendment;[245] (3) the Court contends that the protection will frustrate the important state interest in controlling crime and/or asserts that the protection is irrational, arbitrary, or doctrinally eroded;[246] (4) the Court concludes that the protection should be discarded—either in the category of case at issue or more generally.[247]

All these points are present in Justice Brennan's opinion in *Hayden*, and the basic pattern of analysis is also on display in part or in whole in a broad range of later crime-control opinions—such as *Rodriguez*,[248] *Summers*,[249] and *Sitz*,[250] as well as cases such as *California v. Acevedo*,[251] concerning the search of containers in automobiles and *South Dakota v. Opperman*,[252] concerning inventory search of automobiles. The opinion of the Court in cases such as these repeats variations of the basic argumentative maneuvers found in *Hayden* in order to justify a narrow view of the Fourth Amendment—refusing to recognize in some categories of cases the applicability of traditional Fourth Amendment protections such as the warrant requirement, probable cause, individualized suspicion, or privacy in personal effects. In *Hayden*,

---

[244] Warden v. Hayden, 387 U.S. 294, 301-302 (1967).

[245] *Id.* at 301-02, 309-10.

[246] *Id.* at 302, 306, 308-10.

[247] *Id.*

[248] Illinois v. Rodriguez, 497 U.S. 177 (1990).

[249] Michigan v. Summers, 452 U.S. 692 (1981).

[250] Mich. Dept. of State Police v. Sitz, 496 U.S. 444 (1990).

[251] 500 U.S. 565 (1991).

[252] 428 U.S. 364 (1976).

Justice Brennan and the Warren Court helped to establish and legitimate the analytical framework used to reject many of the basic protections the Fourth Amendment plausibly offers to the people in a broad range of later cases.

Even more important, the Court's complete rejection of the mere evidence rule has very likely had a profound effect on the balancing done under the reframed doctrinal question of "reasonableness," an effect strongly in favor of promoting crime-control policies over individual rights. This is so because the rejection of the mere evidence rule fundamentally changed the doctrinal standing in Fourth Amendment law of individual rights as a counter-weight to crime-control interests. As stated, the mere evidence rule holds that police may not search for mere evidence of a crime even when police have a valid warrant supported by probable cause. The mere evidence rule applies irrespective of the crime under investigation—and thus would bar evidence-gathering searches even in cases of murder, robbery, and rape. The effect of this rule speaks quite clearly for itself: The right to "security" in "protected interests" under the Fourth Amendment trumps even the compelling collective social goal of gathering evidence to prosecute serious crimes such as murder. The traditional mere evidence rule thus represents an uncompromising doctrinal rejection of the Fourth Amendment as a constitutional guarantee that simply balances in a common-sense policy fashion individual interests in privacy against collective interests in crime control—and that may ultimately weigh the balance strongly in favor of the state interest in fighting crime.

It is thus impossible to adhere to the mere evidence rule and also establish a coherent view of Fourth Amendment "reasonableness" that embraces crime-control interests over a broad view of privacy (or liberty)—as the Court does in decisions such as *Rodriguez* and *Sitz*. Both as an informal statement of the Fourth Amendment's underlying values and as a matter of formal stare decisis, the mere evidence rule anchored Fourth Amendment "reasonableness" in a vision which strongly privileges individual rights over the control of crime. Continued adherence to the mere evidence rule, a deeply-rooted doctrine of great significance to the practical operation of the law of search and seizure, would likely have had a substantial influence over time on the views of judicial actors—even on those who ultimately opposed the rule. Fourth Amendment doctrine under the mere evidence rule would have been tied to the "anchoring" message of the rule, reinforced by the doctrine of state decisis, that individual interests broadly trump crime-control interests, not the reverse. The presence of the mere evidence rule thus could have held the Justices to a more rights-protective view of the Fourth Amendment than they have held in its absence.

The explicit and total rejection of the mere evidence rule—premised in part on the need for evidence searches to serve the state interest in suppressing crime[253]—empowered an alternative view of the Fourth Amendment as a mere prohibition of actions by police which are "unreasonable" from a policy perspective emphasizing the suppression of crime. *Hayden* is thus a pivotal precedent and doctrinal enabler for later crime-control decisions on Fourth Amendment "reasonableness" in the Burger and Rehnquist Courts. These later decisions, in turn, have ultimately produced a new anchoring effect on the Fourth Amendment in a strongly crime-control policy direction.

Significantly, the anchoring effects of *Hayden* remain deeply problematic even if the case is correct in some legal sense on the question it decided—whether or not to retain the mere evidence rule.[254] Even if *Hayden* is correct on that question in isolation, the decision nonetheless helped to legitimate and facilitate a revisionist crime-control approach to the Fourth Amendment. That revisionist approach would be invoked within a few years to erode other traditional Fourth Amendment protections—such as the warrant preference, probable cause, and individualized suspicion.

The possible consequences of the *Hayden* decision for Fourth Amendment rights did not go unnoticed at the time the case was decided. Justice Douglas in his dissent appears to have understood the mutually reinforcing facets of the substantive and procedural "zones" of Fourth Amendment protection, and he stated that without the mere evidence rule the Fourth Amendment would become a "ready instrument[ ]" to legitimate invasions of protected interests that the "Framers sought to avoid."[255] Indeed, each post-*Hayden* decision recognizing the "reasonableness" of more forceful and envelope-pushing police conduct—cases such as *Rodriguez* and *Summers* and *Sitz*—reinforces the anchoring of the Fourth Amendment in a crime-fighting policy framework, one in which Fourth Amendment "reasonableness" is equated with a center-right political view of what constitutes reasonable law enforcement behavior.

---

[253] Warden v. Hayden, 387 U.S. 294, 306 (1967).

[254] For instance, some scholars contend that the mere evidence rule does not represent the "original understanding" of the Fourth Amendment. *See* Davies, *supra* note 157. If this view is sound, then from a purely originalist perspective the Court in *Hayden* was right to abrogate the rule.

In an important sense, each decision in favor of a crime-control view of Fourth Amendment "reasonableness" further eases the way for the next case—both in a formal stare decisis sense and in the broader sense of re-anchoring Fourth Amendment doctrine in a crime-control understanding of the proper balance struck within the "reasonableness" frame. Doctrinal evolution is a dynamic process, and the momentum in recent decades has been increasingly with a law-and-order vision of the Fourth Amendment—as the recent cases of *Kentucky v. King*[256] and *United States v. Davis*[257] further illustrate. The framing and anchoring effects of the doctrines are self-reinforcing as later decisions reaffirm—implicitly or explicitly—the "reasonableness" frame and crime-control policy anchor of earlier decisions.

Further, these decisions affect how the broader legal community comes to view the underlying meaning of the Fourth Amendment. Indeed, the common feedback dynamic between constitutional meaning and constitutional doctrine (i.e., the process in which perceptions of constitutional meaning shape the creation of doctrines which in turn over time reshape the original perceptions of meaning) now favors a crime-control "reasonableness" paradigm of the Fourth Amendment as the broader legal community acclimates to the decisions of the Court and that in turn reshapes the community's view of the amendment. As a result, more expansive doctrinal understandings of the Fourth Amendment—whether rooted in earlier historical traditions or in a progressive vision of individual rights—are increasingly marginalized.[258] The Warren Court's wholesale abandonment of the mere evidence rule in *Warden v. Hayden* was an early and crucial step down this path to a much narrower conception of Fourth Amendment freedoms.

---

[255] *Hayden*, 387 U.S. at 325 (Douglas, J., dissenting). The full quotation, with understandable hyperbole, is that "the Fourth Amendment and the Fifth are ready instruments for the police state that the Framers sought to avoid" without the mere evidence rule and the individual choice to protect privacy which it provides. *Id.*

[256] 131 S. Ct. 1849 (2011) (approving a broad range of police-created exigencies as justifications for warrantless searches).

[257] 131 S. Ct. 2419 (2011) (extending the "good faith" exception to the exclusionary rule to reasonable police reliance on binding appellate precedent).

Over forty years after *Hayden*, it would be imprudent to attempt to revive the mere evidence rule as a broad Fourth Amendment doctrine—even if its ultimate merits as a matter of law and public policy seemed otherwise to warrant a restoration, which is certainly subject to debate.[259] Still, the Court could return in part to the rule's underlying vision of the Fourth Amendment—grounded in privileging individual rights over the control of crime—to reinvigorate the protection of Fourth Amendment rights within the Warren Court's established doctrinal framework. This Article will discuss the future of Fourth Amendment reform in more detail in Part V.

V. THE FUTURE OF SECURITY IN PROTECTED INTERESTS: STATUS QUO OR REFORM?

This Article has sketched an account of some of the unintended consequences of the Warren Court's criminal procedure revolution—the ways in which doctrinal innovations that the Court intended to expand the protections of the Fourth Amendment failed to do so and in fact contributed to the ultimate contraction of those protections. What, if anything, should be done about these failures—what is the right way moving forward? This

---

[258] The fact that only Justice Ginsburg dissented in *King* and only Justices Breyer and Ginsburg dissented in *Davis* suggests just how marginalized broader views of the Fourth Amendment and exclusionary rule now are.

[259] For a thoughtful discussion of the merits of a narrow understanding of the mere evidence rule, one limited to its original "paper" search context in *Entick* and *Boyd*, see Cloud, *supra* 213, at 593-98.

Article addresses this question by articulating two plausible reactions to the sketch above both of which seek a practical way forward: an "establishmentarian" response in defense of the status quo and a "reform-minded" response which hopes to reinvigorate the protections of the Fourth Amendment. The author leans decidedly toward the second, while recognizing the power of the first.

The "establishmentarian" response is this: The failure of the Warren Court in this area has not in fact been a bad thing. This is so for a number of related reasons. Constitutional law is an applied science, and it has many moving parts which interact in complex ways: substantive rights, collective social goals, interpretive integrity, and governmental structure. In the face of this practical complexity, constitutional law has to serve real world interests, not the abstract ideals of fast-track progressives or the historical preoccupations of antiquarian conservatives. A Burkean "muddling through"[260] is the best one can hope for, and that approach will routinely achieve a better result than any alternative.

The Court has successfully "muddled through" to a healthy dilution of the rigors of the traditional Fourth Amendment. That dilution is not to be deplored, and it was almost inevitable to offset other overarching legal and social changes. First, the Court's expansion of the Fourth Amendment from a constitutional guarantee limiting only the federal government with its few law enforcement responsibilities to a provision "incorporated" through the Fourteenth Amendment limiting the fifty states with their greater law enforcement responsibilities[261] rendered a dilution of the Fourth Amendment imperative.[262] The Fourth Amendment can severely constrain law enforcement or it can apply to the state governments, but it cannot do both of these at once—at least not without creating an explosion in crime which the American people should not be forced to endure.

---

[260] *See* EDMUND BURKE, REFLECTIONS ON THE REVOLUTION IN FRANCE (1791) (advocating incremental political reform arising organically from a polity's long-standing traditions rather than sudden political change according to abstract rational design).

[261] Mapp v. Ohio, 367 U.S. 643 (1961) (applying the exclusionary rule to the states through the Fourteenth Amendment Due Process Clause); Wolf v. Colorado, 338 U.S. 25 (1949) (applying search and seizure limits associated with the Fourth Amendment to the states through the Fourteenth Amendment Due Process Clause).

[262] *Cf.* Duncan v. Louisiana, 391 U.S. 145, 182 n.21 (Harlan, J., dissenting) (stating that a "major danger of the 'incorporation' [is] that provisions of the Bill of Rights may be watered down" as a result of their application to the states).

Second, the Court's creation of a Fourth Amendment exclusionary rule[263] and the expansion of that rule to the fifty states[264] also necessitated a major dilution in substantive Fourth Amendment protections.[265] If the Court mandates a sweeping rule that "[t]he criminal is to go free because the constable has blundered,"[266] then the Court farther down the road may have to narrow the category of criminal-freeing blunders. One can have a broader Fourth Amendment right with a narrower remedy or one can have a narrower Fourth Amendment right with a broader remedy (such as the exclusionary rule), but one should not expect to have both a broader right and a broader remedy, not with the responsibilities governmental actors have to keep the citizenry safe from crime.

Finally, Fourth Amendment doctrine must reflect the realities of contemporary law enforcement, contemporary (in)tolerance for the harm criminals do to the innocent, and contemporary crime rates. Professionalized police departments, citizens who demand safety, and shifting rates of crime all have consequences for the practical application of the Fourth Amendment which are not captured by the common law of the eighteenth century or the judicial precedents of the nineteenth and early twentieth centuries. Our Constitution was meant "to endure for the ages,"[267] and it must be interpreted to respond to the practical problems one faces today, not the historical problems of past ages or the theoretical problems of social utopians. No one should mourn for the mere evidence rule or the warrant preference. The Court has made its choices, and those choices strike a perfectly reasonable balance among all the competing goals of constitutional law.

---

[263] Weeks v. United States, 232 U.S. 383 (1914).

[264] *Mapp*, 367 U.S. 643.

[265] *Cf. id.* at 681 (Harlan, J., dissenting) (stating that the "Court should continue to forbear from fettering the States with an adamant [exclusionary] rule which may embarrass them in coping with their own peculiar problems in criminal law enforcement").

[266] People v. Defore, 150 N.E. 585, 587 (N.Y. 1926).

[267] McCulloch v. Maryland, 17 U.S. 316, 415 (1819).

The "reform" response is this: The failure of the Warren Court's reframing of Fourth Amendment doctrines has been a bad thing, and it should be a cautionary tale for the next generation of reformers. The rejection of many traditional Fourth Amendment rights over the last several decades is a very serious matter and should be an occasion for careful reflection. In particular, advocates for reform should not allow themselves to be lulled into a false sense of security by familiarity with the Court's current doctrines or by general respect for the authority of the Supreme Court to implement the Constitution.

A "security" in "protected interest" approach to the Fourth Amendment may seem strange today, but that is only because it is no longer the established approach in the courts. A prohibition of "unreasonable" invasions of "reasonable expectations of privacy" would have seemed even stranger to judges, lawyers, and others in, say, 1961. The Supreme Court has now endorsed the new "reasonableness" approach for almost fifty years, but the Court endorsed the traditional approach for at least eighty years before that. Even those persons who define their politics in terms of faith in progress should recognize that newer doctrines are not necessarily better doctrines and that the Warren Court's landmark precedents in any event have now become part of the "dead hand" of the past. To the extent that these newer doctrines have endangered our freedoms, they must be reconsidered.

Even so, uprooting decades of settled law on the hubristic assumption that one can craft something clearly better is also unwise. The Warren Court should not have launched its revolution in criminal procedure, but a counter-revolution to overturn almost a half-century of law built on Warren Court foundations in order to reinstate the traditional "security in protected interests" view could go astray just as easily. Doctrinal reform should be cautious, incremental, and experimental. "Muddling through" in light of the complex interactions of overarching legal and social changes is indeed the right approach and the consequences of constitutional reform for the realities of law enforcement must be carefully considered in each case. Still, the ultimate direction of the "muddling" must be determined, and the right goal is that of providing greater protections for Fourth Amendment rights by returning in part to the earlier foundations of Fourth Amendment doctrine.

How could one achieve that? As suggested, *Kyllo* shows us the most obvious way: Use the nebulous Warren Court "reasonableness" formulations to begin slowly building back into Fourth Amendment doctrine the core protections of the traditional approach reflected in the common law and the pre-Warren Court era.[268] *Kyllo* uses the *Katz* "reasonable expectation of privacy" approach in the context of protections for "houses" but ultimately builds its analysis around the very questions *Katz* rejected—concerning the security of "houses" as constitutionally protected areas against actual physical invasions, an analysis drawn from older cases such as *Silverman*.

The same approach could be used in other areas. One could adhere to the *Katz* "reasonable expectations of privacy" approach in the context of e-mail accounts which are subject to third-party access by Internet Service Providers, but still build the Katzian "reasonableness" analysis on the solid common-law foundations of the traditional protected interest in "papers" as extended to their contemporary digital equivalents.[269] This "reasonable expectation of privacy" could be reoriented toward a respect for traditional "protected interests" which would emphasize the importance of the individual interest in "papers" while rejecting any broad "assumption of the risk" analysis.[270] Consistent with the broader contours of the Katzian doctrines, "reasonable expectations of privacy" can be reframed and re-anchored in part and over time as expectations that are "reasonable" because they reflect the traditional security of protected interests.

---

[268] *See* Cloud, *supra* note 100, at 73 n.144; *cf.* Clancy, *supra* note 52, at 344-66 (advocating that the Court's Fourth Amendment privacy doctrines be reoriented toward a right to be "secure" understood as "the right to exclude the government").

[269] *Cf.* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (recognizing a "reasonable expectation of privacy" in e-mail in part by emphasizing the individual interests at stake given that e-mail is used for "intimate," "sensitive," and "commercial" information and can provide what amounts to an "account of one's life" to government agents who examine it).

[270] *See supra* Part II.

Similarly, one could analyze contemporary Fourth Amendment "reasonableness" cases by emphasizing within the broad outlines of the "reasonableness" frame the more protective analysis of an earlier era. The central focus on the "reasonableness" analysis would pivot on the basic concept of security in protected interests—as Justice Ginsburg reoriented Fourth Amendment "reasonableness" around "security" in her dissent in *Kentucky v. King*.[271] In this fashion, "reasonable" police conduct doctrines under the Fourth Amendment can be carefully reframed and re-anchored—over time and in part—as doctrines mandating that police conduct afford "reasonable security" to protected interests in light of the traditions of the common law and the once well-established procedural limits on governmental searches such as the warrant preference.[272] This partial reframing would reorient the emphasis of the "reasonableness" doctrine around the provision of "security" and the need for compelling police justifications for incursions into protected interests such as the home.

As for the mere evidence rule and the "reasonableness" frame, rather than seek to overrule *Warden v. Hayden* and reinstate the rule in its broad form—overturning almost fifty years of precedent—reformers should aim for a more modest and realistic goal. The Court should act instead merely to discredit the perfunctory application of *Hayden*'s argumentative framework to eviscerate traditional Fourth Amendment protections and to revive something of the animating spirit behind the mere evidence rule, one which recognizes that the Fourth Amendment is designed to protect the rights of the people even at substantial cost to the interests of law enforcement. Thus a partial revival of the mere evidence rule—emphasizing its spirit rather than its formal letter—to inform the application of Fourth Amendment "reasonableness" represents the best path forward.[273]

---

[271] 131 S. Ct. 1849, 1864-66 (2011) (Ginsburg, J., dissenting).

[272] Johnson v. United States, 333 U.S. 10, 14 (1948).

[273] The Court might also carefully consider a revival of the "paper" search aspect of the rule—barring evidence searches of personal papers but not other forms of property. *See* Cloud, *supra* note 213.

Scholars, lawyers, and others could work to maximize the appeal of these gradual and partial doctrinal reorientations by defending their grounding in law and policy as broadly as possible. The argument for doctrinal reorientation could be grounded in the Anglo-American common-law constitutional tradition to appeal to historically-oriented judicial conservatives, and the argument could also be grounded in a progressive vision of the rights of the people to appeal to policy-oriented judicial liberals. A conservative-liberal coalition of precisely this sort produced the majority opinion in *Kyllo*[274] and has also produced recent decisions affirming a broadly protective view of individual rights under the Sixth Amendment in cases involving both the right to jury trial[275] and the right to confront witnesses.[276] Such a coalition has the best promise both to succeed in the nearer run and to do so with the kind of broad legitimacy that is likely to preserve its successes over time.[277] In short, an incrementalist and coalition-building approach is the most plausible path to "muddling through" to a better world. No doubt it will be an uphill struggle, but rebuilding the Fourth Amendment on stronger foundations is an important reform goal well worth the effort.

---

[274] The *Kyllo* majority consisted of Justices Scalia, Thomas, Souter, Ginsburg, and Breyer. Kyllo v. United States, 533 U.S. 27 (2001).

[275] *See* Blakely v. Washington, 542 U.S. 296 (2004) (holding that any fact used to increase a defendant's sentence above the statutory maximum must be submitted to a jury and proved beyond a reasonable doubt). The *Blakely* majority consisted of Justices Scalia, Stevens, Souter, Thomas, and Ginsburg. *Id.*

[276] *See* Bullcoming v. New Mexico, 131 S. Ct. 2705 (2011) (holding that the Confrontation Clause guarantees the basic right of a criminal defendant to confront an analyst who certifies a forensic laboratory report containing a testimonial certification introduced by the prosecution to prove a fact at a criminal trial). The *Bullcoming* majority consisted of Justices Ginsburg, Sotomayor, Kagan, Scalia, and Thomas. *Id.*

[277] Conservative Justices in recent years have also expressed support in other cases for a broad view of individual rights on historical grounds which converge substantively with views adopted by some liberal Justices as a broader matter of law and public policy. For instance, Justice Thomas, on originalist grounds, has expressed sympathy for the view that suspicionless stops at roadway checkpoints are impermissible. City of Indianapolis v. Edmond, 531 U.S. 32, 56 (2000) (Thomas, J., dissenting). Justice Brennan endorsed the same ultimate position in *Sitz.* Mich. Dept. of State Police v. Sitz, 496 U.S. 444, 456 (1990) (Brennan, J., dissenting). Further, Justice Thomas—joined by Justice Scalia—has also expressed some support for a broad view of the Fifth Amendment Self-Incrimination Clause that would extend the provision's protections from compelled testimonial evidence to compelled production of physical evidence. Justice Thomas states that a "substantial body of [historical] evidence suggests that the Fifth Amendment privilege protects against the compelled production not just of incriminating testimony, but of any incriminating evidence." United States v. Hubbell, 530 U.S. 27, 49 (2000) (Thomas, J., concurring). This view is similar to that endorsed by Justice Black—joined by Justice Douglas—in *Schmerber*,

CONCLUSION

The characteristic failing of the Warren Court was disregard for constitutional tradition: the traditional role of the Court, traditional methods of legal interpretation, traditional respect for the authority of political institutions, and traditional rights. The American constitutional tradition—a living tradition,[278] as Justice Harlan, the "great dissenter" of the Warren Court,[279] put it when describing the doctrine of substantive due process—strikes a prudent balance between historical constitutional constraint and openness to constitutional change. That tradition is the best vehicle for adapting the Constitution to changing times—and the changing times to the Constitution. Rather than build on this tradition, the Warren Court's revolution in criminal procedure improvidently abandoned it—shattering the Fourth Amendment's doctrinal structure built on the solid rock of history and leaving the amendment resting precariously on the shifting sands of policy analysis.

The Warren Court's attempt to expand the protections of the Fourth Amendment by reframing its doctrines as open-ended "reasonableness" tests has failed and has left the amendment's protections unsure and subject to increasingly narrow interpretations. The doctrinal shifts from enumerated "protected interests" to "reasonable expectations of privacy," from Fourth Amendment "security" to the mere "reasonableness" of police conduct, from the mere evidence rule providing substantive

---

arguing that the Fifth Amendment right against self-incrimination should be read broadly to protect an individual from state compulsion to submit to a blood alcohol test to collect physical evidence of driving under the influence of an intoxicant. Schmerber v. California, 384 U.S. 757, 773-78 (1966) (Black, J., dissenting).

[278] Poe v. Ullman, 367 U.S. 497, 542 (1961) (Harlan, J., dissenting).

[279] *See* TINSLEY E. YARBROUGH, JOHN MARSHALL HARLAN: GREAT DISSENTER OF THE WARREN COURT (1992). Notably, Justice Harlan, the "great dissenter," concurred in *Katz* and joined the opinion of the Court in *Hayden*.

Fourth Amendment protections to facilitating the law enforcement interest in "solving crime"[280] have all rendered Fourth Amendment rights less certain and less secure. As the Thomas More portrayed in *A Man for All Season*'s might put it, the Warren Court cut down the laws to get at a devil—aggressive policing—and the Court's liberal Justices in turn found no laws left to protect our rights when the devil turned and new political winds began to blow.[281]

The Court's contemporary Fourth Amendment doctrines descend from the Warren Court era, and the temptation to acclimate to them—to accept them as simply defining the legitimate mainstream of American criminal procedure and as marginalizing more protective views of the Fourth Amendment rooted in past traditions or in a progressive vision of the future—should be resisted. The obvious way forward to reinvigorate the protections of the Fourth Amendment is through a cautious, incremental, and partial restoration of the core of the amendment's traditional protections within the doctrinal framework established by the Warren Court. The best hope to achieve this goal is through an appeal to a potential conservative-liberal coalition, one wedded to the all-important nexus between respect for our older legal traditions and the "rights of the people" which justice demands. If we are to rebuild Fourth Amendment doctrine on a more solid foundation, that is the most promising path.

---

[280] Warden v. Hayden, 387 U.S. 294, 306 (1967).

[281] ROBERT BOLT, A MAN FOR ALL SEASONS 56 (1954). The relevant scene reads:

> ROPER. So now you'd give the Devil benefit of law.
>
> MORE, *turning to Roper*. Yes. What would you do? Cut a great road through the law to get after the Devil?
>
> ROPER. I'd cut down every law in England to do that!
>
> MORE, *roused and excited*. Oh? And when the last law was down—(*He moves to r. of Roper.*) and the Devil turned round on you—where would you hide, Roper, the law's all being flat? (*He crosses to L.C.*) This country's planted thick with laws from coast to coast—Man's laws, not God's—and if you cut them down—and you're just the man to do it—you really think you could stand upright in the winds that would blow then? (*Quietly.*) Yes, I'd give the Devil benefit of law, for my own safety's sake.

Id.

RESPONDING TO THE CHALLENGES OF CONTEXTUAL CHANGE AND LEGAL DYNAMISM IN INTERPRETING THE FOURTH AMENDMENT

*Donald A. Dripps**

INTRODUCTION 1086
I. SPECIFIC PRACTICE ORIGINALISM 1090
II. THE CONTEXTUAL CRITIQUE 1094
  A. The Criminal Justice System in 1791 1094
  B. The Sweeping Changes in the Nineteenth Century 1097
  C. The Contextual Critique of SPO 1101
    1. Founding-Era Application Understandings...1102
    2. Founding-Era No-Application Understandings...1117
III. THE DYNAMISM CRITIQUE..1121
  A. Judicial Changes in Common-Law Doctrine 1122
  B. Statutory Revisions of Common-Law Rules 1124
IV. DESCRIPTIVE BALANCE OF ADVANTAGE ACCOUNTS: ANALYSIS AND CRITIQUE.....................................1126
  A. The Balance of Advantage Concept 1126
  B. Descriptive Balance-of-Advantage Accounts: A Critique 1127
IV. ASPIRATIONAL BALANCE OF ADVANTAGE ORIGINALISM...1128
CONCLUSION 1131

---

* Professor, University of San Diego School of Law. Thanks to Tom Clancy and the University of Mississippi National Center for Justice and the Rule of Law for organizing the excellent symposium on The Fourth Amendment: Current Analysis, Views of the Future, and Digital Searches and Seizures on March 9-11, 2011. This article is much improved as a result of what I learned there.

INTRODUCTION

Our topic is what makes a search or seizure reasonable under the Fourth Amendment. The positive law on this point has become formulaic. First, we ask, under the *Edmond* and *Ferguson* cases, whether the government's primary purpose is criminal prosecution or something else.[1] If the answer is "something else" we engage in a multi-factor balancing process, taking account of the degree of intrusiveness on individual liberty or privacy, the weight of the government's interest, the requirement *vel non* of individualized suspicion, aspects of voluntarism, and so on.[2]

If the answer is "criminal prosecution," we first must characterize the Fourth Amendment event as a temporary detention under *Terry*, an arrest, or a free-standing search for evidence or contraband. A *Terry* stop is "reasonable" without judicial authorization given "articulable facts" short of "probable cause."[3] An "arrest" by contrast is always unreasonable without "probable cause,"[4] and entry into private premises to effect an arrest requires prior judicial authorization subject to such exceptions as emergency and consent.[5] A "search" for evidence, unconnected to arrest or *Terry*-type detention, is presumed unreasonable absent probable cause and a warrant.[6] Consent is an exception to both requirements,[7] while exigency, search incident to arrest, and vehicle searches are recognized as exceptions to the warrant requirement.[8]

---

[1] Ferguson v. City of Charleston, 532 U.S. 67, 84-86 (2001) (holding urinalysis program unconstitutional because directed towards generating evidence for law enforcement purposes); City of Indianapolis v. Edmond, 531 U.S. 32, 48 (2000) (holding checkpoint program unconstitutional because it served no need beyond traditional law enforcement purposes).

[2] *See, e.g.*, Cassidy v. Chertoff, 471 F.3d 67 (2d Cir. 2006) (rejecting Fourth Amendment challenge to suspicionless searches of passenger luggage on Lake Champlain ferry).

[3] *See, e.g.*, Alabama v. White, 496 U.S. 325, 330 (1990) ("Reasonable suspicion is a less demanding standard than probable cause not only in the sense that reasonable suspicion can be established with information that is different in quantity or content than that required to establish probable cause, but also in the sense that reasonable suspicion can arise from information that is less reliable than that required to show probable cause."); Illinois v. Gates, 462 U.S. 213, 238 (1983) (affirming that probable cause is tested by asking whether under "the-totality-of-the circumstances . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place"); Allen v. City of Los Angeles, 66 F.3d 1052, 1056 (9th Cir. 1995) (plaintiff contends "that the methods the defendants used to detain him converted the initially lawful *Terry* stop into a full-fledged arrest for which probable cause was required, but was lacking . . . ." There is, however, "no bright line rule for determining when an investigatory stop crosses the line and becomes an arrest.").

[4] *See* Dunaway v. New York, 442 U.S. 200, 208-09 (1979) ("The [probable cause] standard applied to all arrests, without the need to 'balance' the interests and circumstances involved in particular situations.").

The Supreme Court sometimes has looked to founding-era common law to determine whether contested police actions were reasonable or unreasonable.[9] Granting for purposes of argument the general theoretical case for interpreting the constitutional text according to some version of the original understanding, my thesis is that consulting founding-era practices at this level of particularity is not a faithful approach to the original understanding. I develop two lines of objection to specific-practices originalism (SPO). I call one the contextual critique and the second the dynamism critique.

---

[5] Payton v. New York, 445 U.S. 573 (1980) (holding that Fourth Amendment requires a warrant to enter the suspect's home absent exigency, "hot pursuit" or consent).

[6] *See, e.g.*, Ferguson v. City of Charleston, 532 U.S. 67, 86 (2001) ("The Fourth Amendment's general prohibition against nonconsensual, warrantless, and suspicionless searches necessarily applies to [the city's drug-testing] policy."); Kyllo v. United States, 533 U.S. 27, 40 (2001) (where agents obtained search warrant in part based on results of thermal-imager scan of defendant's home, the Court held thermal-imager's use constituted a search and remanded the case "to determine whether, without the evidence it provided, the search warrant issued in this case was supported by probable cause . . . ."); Bond v. United States, 529 U.S. 334 (2000) (holding that agent's groping of bus passenger's bag was a search in violation of the Fourth Amendment). The *Bond* Court did not say whether the "search" was illegal for want of probable cause or for want of a warrant. The opinions have not foreclosed the possibility that some "search" for evidence of crime outside the home might be justified on less than probable cause. The vehicle-search cases, however, excuse only the failure to obtain a warrant, not the absence of probable cause. Similarly, during a valid *Terry* stop, the police may "pat down" the suspect for weapons but not engage in a general search for evidence of the sort allowed incident to arrest. *See, e.g.*, Minnesota v. Dickerson, 508 U.S. 366, 373 (1993) ("If the protective search goes beyond what is necessary to determine if the suspect is armed, it is no longer valid under *Terry* and its fruits will be suppressed." (citation omitted)).

[7] *See, e.g.*, Illinois v. Rodriguez, 497 U.S. 177 (1990) (upholding warrantless home search based on consent from individual with apparent but not actual authority to permit entry).

[8] There are multiple exceptions, see, for example, Craig Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1473-74 (1985) (identifying "over twenty exceptions"), but the exceptions listed in text are the ones commonly seen in litigation. *See id.* at 1475 ("As anyone who has worked in the criminal justice system knows, searches conducted pursuant to these exceptions, particularly searches incident to arrest, automobile and 'stop and frisk' searches, far exceed searches performed pursuant to warrants." (footnote omitted)).

[9] *See infra* Part I.

The constitutional text was situated in the context of eighteenth-century institutions and doctrines that disappeared in the nineteenth century. The utter disappearance of the context means that we just don't know what the founders expected the Fourth Amendment to prohibit, or permit, in a radically different legal and technological environment. The degree of privacy and liberty in 1791 were a product of the contemporary criminal justice system, the economic and technological social circumstances, and the legal regime that limited search-and-arrest powers. Rules in 1791 had different consequences for liberty and security than those rules would have in a society like today's, with full-time proactive police and modern technology.

The dynamism critique points out that the 1791 rules of search-and-seizure were not static. Tort law was the legal regime regulating search-and-arrest powers. Illegal detention gave rise to actions for false arrest or false imprisonment. Illegal entries of private premises gave rise to trespass suits. But common law can change. Precedents can be overruled, and new factual contexts require debatable applications of old principles. Most dramatically, common-law rules can be trumped by statutes.

If the reasonableness clause perpetuates *all* the specific 1791 tort rules, the force of the contextual critique becomes overwhelming. If, however, the clause incorporates common-law rules subject to plenary statutory revision, the constitutional provision is nugatory. Either the Fourth Amendment freezes search-and-seizure law in the form it had before the advent of modern police and modern technology, or it permits any search or arrest authorized by statute. Some search for principled middle ground seems in order.

Kyllo v. United States[10] gives the most plausible accommodation yet of originalism against the contextual critique.

---

[10] 533 U.S. 27 (2001).

Justice Scalia's majority opinion in *Kyllo* read the Fourth Amendment as instantiating the degree of liberty and security enjoyed against government as of 1791.[11] This move surrenders specific-practice originalism in favor of an under-determined abstraction; it counters the contextual critique by surrendering some of the determinacy that makes originalism attractive in the first place.

Selecting the 1791 level of privacy and liberty, however, is arbitrary, because we have no reason to believe that those who ratified the Fourth Amendment believed the prevailing balance of liberty and security was ideal. In fact, the founders themselves tinkered with the common law of crimes and criminal procedure on an extensive scale.[12] Indeed, to actually restore the level of individual security that prevailed in 1791 would require abolishing modern police. Leaving aside the modern unthinkability of that notion, we have no reason to suppose that the founders would have thought a professional, proactive force as such was a violation of the Fourth Amendment.

We should not assume the founders meant to perpetuate the 1791 common law of torts against either statutory or judge-made changes, whether those changes favor the liberty of the citizen or the security of the public. The most that can be hoped for is to steer the messy body of precedents so as to achieve and maintain something resembling the overall balance of advantage between individual freedom and public security that we think the founders *would have wished* if they had faced the dangers and opportunities of the modern world. I call this approach "aspirational balance of advantage originalism" and frankly concede that it is less than a completely determinate theory. Indeed, given even some modest regard for precedent and some sense of legal tradition, the difference between treating "unreasonable searches and seizures" as incorporating modern values by reference, and treating that phrase as a term of art with some technical content, becomes so slight as to be of doubtful practical relevance.

---

[11] *Id.* at 33-34. The Court's most recent Fourth Amendment decision returned to *Kyllo*'s descriptive balance-of-advantage standard. *See* United States v. Jones, 132 S. Ct. 945, 950 (2012) ("At bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (quoting *Kyllo*, 533 U.S. at 28)).

[12] *See infra* Part III.B.

So we proceed in four stages. First, we take SPO as our point of departure, briefly discussing the various Supreme Court decisions that have looked to 1791 rules as defining "unreasonable searches and seizures." Second, we develop the contextual critique. We describe the eighteenth-century criminal justice system and the sweeping institutional and doctrinal changes to that system in the nineteenth century. We then explain how these massive contextual changes make specific founding-era rules and practices at best inconclusive guides to the original understanding.

Third, we develop the dynamism critique. The common-law regulating search and seizure was understood to be subject to revision by both courts and legislatures. The founders themselves departed from the common-law system in numerous ways, including modifying the search-and-seizures rules. Fourth, we turn to balance-of-advantage accounts and defend the aspirational balance of advantage theory as the most attractive originalist formulation of the Fourth Amendment.

I. SPECIFIC PRACTICE ORIGINALISM

The Supreme Court's clearest articulation of SPO appears in *Wyoming v. Houghton.*[13] The issue before the Court was whether police making a warrantless search of an automobile could look inside private containers (a purse and then a wallet) that might contain the suspected contraband. The Court, following prior cases, held the search reasonable.[14] For our purposes, the interesting part of Justice Scalia's majority opinion is the interpretive method it adopts:

> [W]e inquire first whether the action was regarded as an unlawful search or seizure under the common law when the Amendment was framed. Where that inquiry yields no answer, we must evaluate the search or seizure under

---

[13] 526 U.S. 295 (1999).

[14] *Id.* at 306-07.

> traditional standards of reasonableness by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.[15]

This approach reads the reasonableness clause as adopting by reference the common-law tort limits on law enforcement that prevailed at the founding.

This precise formulation has not guided all of the Court's Fourth Amendment cases. It has been criticized as an eccentric outlier,[16] but remains important enough to be taken seriously, for two reasons. First, reading "unreasonable searches and seizures" as a term of art incorporating the body of common-law tort rules enjoys weighty support in the historical record.[17] Second, the Court has followed this approach in a significant number of important cases over the years.

The Court has followed the *Houghton* formula in three more cases.[18] In each of these cases, the Court concluded that the citizen failed to establish that the search or arrest violated 1791 common law.[19] Proceeding then to the second prong of the *Houghton* formula, the Court then ruled for the prosecution or the police after a balancing of interests.[20]

---

[15] *Id.* at 299-300 (citations omitted).

[16] THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 507-09 (2008).

[17] Perhaps the most thorough historical study reaches just this conclusion. *See* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 602-1791, at 739-58 (2009); *cf.* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547 (1999) (arguing that the Fourth Amendment prohibits general warrants and not any larger category of "unreasonable searches"). My current view is that reasonableness was thought to be a limit on search powers distinct from the ban on general warrants, in part, because of the evidence marshaled by Cuddihy, *see* CUDDIHY, *supra*, at 777-82 (criticizing Davies), and in part, because the text itself points so strongly in that direction. If Davies is right and Cuddihy is wrong, however, *all* of the Court's reasonableness decisions are off on the wrong historical foot, before they ever reach the question of just what makes a search reasonable.

[18] *See* Virginia v. Moore, 553 U.S. 164, 168 (2008) ("We look to the statutes and common law of the founding era to determine the norms the Fourth Amendment was meant to preserve."); Atwater v. City of Lago Vista, 532 U.S. 318, 326-27 (2000) ("[T]he first step here is to assess Atwater's claim that peace officers' authority to make warrantless arrests for misdemeanors was restricted at common law . . . ."); Florida v. White, 526 U.S. 559, 563 (1999) ("In deciding whether a challenged governmental action violates the Amendment, we have taken care to inquire whether the action was regarded as an unlawful search and seizure when the Amendment was framed." (citing Wyoming v. Houghton, 526 U.S. 295, 299 (1999); Carroll v. United States, 267 U.S. 132, 149 (1925))).

SPO, however, has a long, if chequered, pre-*Houghton* history. In *Boyd v. United States*, the Court struck down a federal statute that required production of business records that were not themselves contraband.[21] The *Boyd* Court reasoned that the founders expected the Fourth Amendment to prohibit warrants other than those known to the common law, namely, warrants to arrest and to search for stolen goods.[22] In particular, *Boyd* read the English decision in *Entick v. Carrington* to prohibit the seizure of private papers for evidentiary use, even if the seizure was authorized by a specific warrant.[23]

In *Carroll v. United States*,[24] the Court analogized automobile searches to warrantless searches of ships for undutied goods, a practice authorized by the First Congress and so intended as an instance of the Fourth Amendment's *no*-application.[25] In *Olmstead v. United States*,[26] the Court held that wiretapping was not a "search" because the Fourth Amendment protects only "persons, houses, papers and effects."[27] Absent a common-law trespass, there was no search at all.[28]

---

[19] *See Moore*, 553 U.S. at 170-71; *Atwater*, 532 U.S. at 336; *White*, 526 U.S. at 564.

[20] *See Moore*, 553 U.S. at 171; *Atwater*, 532 U.S. at 354; *White*, 526 U.S. at 566.

[21] 116 U.S. 616 (1886).

[22] *Id.* at 622-23.

[23] *See id.* at 626-29 (quoting extensively from *Entick v. Carrington*, 19 How. St. Tr. 1029, 95 Eng. Rep. 807 (C. P. 1765)). The *Boyd* Court concluded:

> Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony, or of his private papers to be used as evidence to convict him of crime, or to forfeit his goods, is within the condemnation of that judgment [in *Entick*].

Id. at 630.

[24] 267 U.S. 132 (1925).

[25] *See id.* at 149-54.

[26] 277 U.S. 438 (1928).

[27] *Id.* at 465.

[28] *See id.* at 464 ("There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.").

Those who follow Fourth Amendment jurisprudence will realize why I call SPO's history "chequered." *Boyd* and *Olmstead* have been overruled, and there is little discernible sympathy for a return to either.[29] Yet neither *Katz*, which overruled *Olmstead*, nor *Fisher* and *Doe*, which overruled *Boyd*, engage in any serious effort to show that the *Boyd* or *Olmstead* Courts were mistaken in their respective histories.

SPO has guided the analysis in several more modern pre-*Houghton* cases. In *United States v. Watson*,[30] the Court took the view that warrantless felony arrests were permitted because the Fourth Amendment adopted the common-law arrest rules.[31] More recently, in *Wilson v. Arkansas*, the Court held that the Fourth Amendment bans execution of warrants except in compliance with founding-era common law's knock-and-announce requirement.[32]

On its face, SPO seems perfectly plausible. The general phrase "unreasonable searches and seizures" references searches and seizures that would have been actionable at common law, or contrary to statute, as of 1791. Professor Sklansky's important criticism, that on many important issues the common law of 1791 was uncertain, either because there were no authorities or because the available authorities disagreed,[33] leads to *Houghton*'s second step. If no common-law consensus was established in 1791, the Court then balances interests in the spirit of American traditions.

---

[29] *See* United States v. Doe, 465 U.S. 605, 618 (1984) (O'Connor, J., concurring) ("The notion that the Fifth Amendment protects the privacy of papers originated in *Boyd* . . . but our decision in *Fisher v. United States* sounded the death-knell for *Boyd*. 'Several of *Boyd's* express or implicit declarations [had] not stood the test of time[,]'and its privacy of papers concept '[h]ad long been a rule searching for a rationale . . . .' Today's decision puts a long-overdue end to that fruitless search." (citations omitted)); Katz v. United States, 389 U.S. 347 (1967) (overruling *Olmstead*).

[30] 423 U.S. 411 (1976).

[31] *See id.* at 418 ("The cases construing the Fourth Amendment thus reflect the ancient common-law rule that a peace officer was permitted to arrest without a warrant for a misdemeanor or felony committed in his presence as well as for a felony not committed in his presence if there was reasonable ground for making the arrest." (citations omitted)).

[32] 514 U.S. 927, 929 (1995) ("[W]e hold that this common-law 'knock and announce' principle forms a part of the reasonableness inquiry under the Fourth Amendment.").

[33] David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739 (2000).

I now develop two critiques of SPO even in those cases in which a definite 1791 rule or practice can be identified. The contextual critique points out that specific founding-era rules or practices have very different consequences in the criminal justice system that developed after the founding. The dynamism critique suggests that no informed and thoughtful person could have expected the common law of 1791, as it pertained to searches and seizures, to remain unchanged for decades, let alone centuries.

II. THE CONTEXTUAL CRITIQUE

A. The Criminal Justice System in 1791

There were no police of the modern type in colonial America. Sheriffs and constables executed warrants and could organize a posse in the face of armed resistance. There was a night watch.[34] There was, however, no round-the-clock professional force to keep order, and even if such a force existed, communications were too slow to have made it much use.

When a surly Boston crowd confronted a British sentry outside the customs house in March 1770, they were confronted by a stick-toting member of the watch, Edward Langford.[35] All Langford could do at the time was urge the crowd to disperse, with predictable futility.[36] Afterward Langford testified at one of the murder trials arising from the so-called Boston Massacre.[37] He had been converted from law officer to spectator by a crowd armed with snowballs, clubs, and oyster shells.[38] The military could disperse such a mob, but only by indulging, literally, in overkill. So British law forbade the military to fire on civilians until a justice of the peace had read the Riot Act.[39]

---

[34] For a description of the constable-night watch system, see JOEL SAMAHA, CRIMINAL JUSTICE 139 (7th ed. 2006).

[35] The standard account of the Boston Massacre remains HILLER B. ZOBEL, THE BOSTON MASSACRE (1970).

[36] *See* 3 LEGAL PAPERS OF JOHN ADAMS 108 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965) (recording Adams' notes of Langford's testimony).

[37] *Id.*

[38] For an account of the confrontation, see ZOBEL, *supra* note 35, at 203.

[39] *See* 4 WILLIAM BLACKSTONE, COMMENTARIES *144 (describing the Riot Act adopted during the reign of George I).

Neither the watch nor the military had any established role in investigating suspected offenses. That mission was lodged in the justices of the peace and in the grand jury. From what we know of the common-law practice in the age of Blackstone, the typical felony prosecution originated with a complaint by the victim (or the victim's next of kin).[40] As Peter King's study of property crime in Essex County documents, a formal complaint to the justice of the peace might not happen for a variety of reasons.[41] The offender might never be identified or apprehended; the victim might reach an accommodation with the offender; or the victim might not have the time, money, or taste for risking retaliation.[42]

The formal process would be launched only absent these contingencies. The private prosecutor would describe the case to the justice of the peace.[43] If the arrest were not already accomplished, the justice of the peace could issue an arrest warrant.[44] The justice of the peace would then take sworn statements from the witnesses and put them under recognizance to appear at the next court session, to be heard by the grand jury, and if necessary, at the trial.[45]

---

[40] For a knowledgeable overview of the extensive historiography, see Bruce P. Smith, *English Criminal Justice Administration, 1650-1850: A Historiographic Essay*, 25 LAW & HIST. REV. 593 (2007). *See also* PETER J. KING, CRIME, JUSTICE, AND DISCRETION IN ENGLAND 1740-1820, at 17 (2001) ("It was the victim who provided the momentum, the driving force that moved a dispute towards a trial in the major courts.").

[41] KING, *supra* note 40, at 17 (2001) ("It was the victim who provided the momentum, the driving force that moved a dispute towards a trial in the major courts.").

[42] *Id.*

[43] On the English practice of private prosecutions, which continued in that country until late into the nineteenth century, see JAMES FITZJAMES STEPHEN, 1 A HISTORY OF THE CRIMINAL LAW OF ENGLAND 493-99 (1883); Norma Landau, *Indictment for Fun and Profit: A Prosecutor's Reward at Eighteenth Century Quarter Sessions*, 17 LAW & HIST. REV. 507 (1999); and Paul Rock, *Victims, Prosecutors and the State in Nineteenth Century England and Wales*, 4 CRIM. JUST. 331 (2004). For some qualifications, see Smith, *supra* note 40, at 620-21. Another caveat is that after the establishment of the Metropolitan Police, police officers prosecuted the cases they had investigated. *See* WILBUR R. MILLER, COPS AND BOBBIES: POLICE AUTHORITY IN NEW YORK AND LONDON, 1830-1870, at 74-75 (1977).

[44] The range of options open to the justice of the peace after arrest is illuminated by Peter King's study of the property-offense prosecutions in Essex County. *See* KING, *supra* note 40, at 82-125 (2000). Prior to contact with the justice of the peace, there could be, and often were, negotiations and settlements between victims and offenders.

Once arrested, the prisoner would be brought before the justice of the peace for examination.[46] The prisoner, unlike other witnesses at these pretrial examinations, was not sworn.[47] The tenor of the so-called Marian statutes authorizing the examination suggests that the justice of the peace had no discretion to discharge the prisoner, and the leading justice of the peace manuals suggest as much.[48] On the other hand, Blackstone stated that if at examination it "manifestly appears" that no crime had been committed, or that the suspicion against the prisoner was

---

[45] *Id.*

[46] The preliminary examination in English law arose from the so-called Marian statutes, the bail statute of 1554-1555, and the committal statute adopted in 1555. The seminal study of these statutes and the practice under them is JOHN H. LANGBEIN, PROSECUTING CRIME IN THE RENAISSANCE: ENGLAND, GERMANY, FRANCE (1974). For the text, and context, of the statutes themselves, see *id.* at 5-20. The basic procedure was described as follows:

> WHEN a delinquent is arrested by any of the means mentioned in the preceding chapter, he ought regularly to be carried before a justice of the peace. And how he is there to be treated, I shall next shew, under the second head, of commitment and bail.
>
> THE justice, before whom such prisoner is brought, is bound immediately to examine the circumstances of the crime alleged : and to this end by statute 2 & 3 Ph. & M. c. 10. he is to take in writing the examination of such prisoner, and the information of those who bring him : which, Mr. Lambard observes a, was the first warrant given for the examination of a felon in the English law. For, at the common law, nemo tenebatur prodere seipfum ; and his fault was not to be wrung out of himself, but rather to be discovered by other means, and other men. If upon this enquiry it manifestly appears, either that no such crime was committed, or that the suspicion entertained of the prisoner was wholly groundless, in such cafes only it is lawful totally to discharge him. Otherwise he must either be committed to prison, or give bail; that is, put in securities for his appearance, to answer the charge against him.

BLACKSTONE, *supra* note 39, at *293-94 (footnotes omitted).

[47] *See* Eben Moglen, *Taking the Fifth: Reconsidering the Origins of the Constitutional Privilege Against Self-Incrimination*, 92 MICH. L. REV. 1086, 1098 (1994) ("All sources agreed on three critical points: (1) at the preliminary examination, the defendant was to be questioned unsworn; (2) his statements were to be made a matter of formal written record; and (3) his confession, if any, was to be admissible against him at trial.").

[48] LANGBEIN, *supra* note 46, at 47 n.81.

"wholly groundless," in "such cases only it is lawful to totally discharge him."[49]

If the justice of the peace committed the prisoner, bail ordinarily would be denied in felony cases.[50] Gaol conditions were dreadful.[51] The character of eighteenth-century pretrial detention can be inferred from the practice of holding court sessions in the open air, thereby reducing the stench to tolerable levels.[52] Those without friends to pay "fees" to the gaolers for such services as clothing and the removal of irons likely suffered the most from gaol conditions.[53]

B. The Sweeping Changes in the Nineteenth Century

In 1790, Philadelphia undertook the first experiment with the penitentiary system by converting space at the Walnut Street Jail into a "penitentiary house" for "hardened and atrocious offenders."[54] The first full-blown experiments took place decades later, at Auburn in New York in the 1820s[55] and then with the opening of Eastern State Penitentiary at Cherry Hills, Pennsylvania in 1829.[56] By the end of the century, the penitentiary had become the standard penalty for serious crimes. Capital punishment was confined almost exclusively to murder and rape, and as early as 1792 Pennsylvania made some murder punishable by imprisonment.[57] In 1846 Michigan abolished the death penalty altogether.[58]

---

[49] BLACKSTONE, *supra* note 33, at *294.

[50] LANGBEIN, *supra* note 46, at 48-49. Blackstone says that felonies are bailable at common law, but then lists a long sequence of statutes barring bail for almost all felony cases. BLACKSTONE, *supra* note 39, at *295-97.

[51] *Id.* at 49.

[52] *Id.* at 50.

[53] On the practice of charging such fees, see JOHN HOWARD, THE STATE OF THE PRISONS IN ENGLAND AND WALES, at 25-27 (1777), *available at* http://books.google.com/books?id=4EhNAAAAYAAJ&printsec=frontcover&dq=john+howard+state+of+the+prisons&hl=en&ei=6fNpTP6ZKof6sAOX7Y2DBw&sa=X&oi=book_result&ct=result&resnum=2&ved=0CDEQ6AEwAQ#v=onepage&q&f=false.

[54] TODD R. CLEAR, GEORGE F. COLE & MICHAEL D. REISIG, AMERICAN CORRECTIONS 44 (9th ed. 2009).

[55] *Id.* at 45.

[56] *Id.*

This change in the output of the criminal justice system had profound implications for the rest of the system. The common-law criminal process was full of escape-hatches such as hypertechnical pleading requirements, jury nullification, benefit of clergy, and pardons, all designed to defeat the actual infliction of capital punishment on minor offenders.[59] These devices were highly successful. For 1791, the most comprehensive database available records only eleven executions in the United States: seven for murder, two for forgery, and one each for rape and for burglary.[60] With the de jure decline of capital punishment, it became possible to rationalize the criminal process for the purpose of finding the truth rather than concealing it.

The growth of urban crime, including genuine riots, could not be contained by the old watch system. "The usual criticisms" of the watchmen "were they slept when they should have been watching; they shook their 'rattles' only to scare off criminals rather than apprehending them; and they ran away from real danger."[61] In New York, for example:

> [W]ild young men about town . . . thought that a night's spree would not be appropriately ended except they had played some practical joke on the City Watch, which took

---

[57] *See* STUART BANNER, THE DEATH PENALTY: AN AMERICAN HISTORY 97 (2002) ("Pennsylvania's 1786 penal reform, the first of many that would follow in the United States over the course of the next century, abolished capital punishment for robbery, burglary, sodomy, and buggery."); *id.* at 98 ("Between 1794 and 1798 five states abolished the death penalty for all crimes other than murder, and three of the five even abolished it for certain kinds of murder. The first was Pennsylvania, which in 1794 provided prison sentences in place of death for treason, manslaughter, rape, arson, and counterfeiting. Murder remained the sole capital crime, and even murder, for the first time in any jurisdiction with a legal system based on that of England, was divided into degrees . . . . Two years later Virginia enacted a similar statute.").

[58] Rhode Island (1852) and Wisconsin (1853) followed. *Id.* at 134.

[59] *See, e.g.*, Michael Tonry, *Mandatory Penalties*, *in* 16 CRIME AND JUSTICE: A REVIEW OF RESEARCH 247-49 (M. Tonry ed., 1992) (discussing these response to mandatory death penalties in Britain).

[60] *Executions in the United States, 1608-2002: The ESPY File*, DEATH PENALTY INFORMATION CENTER *available at* http://www.deathpenaltyinfo.org/documents/ESPYyear.pdf.

[61] SAMAHA, *supra* note 34, at 139.

> the form generally of upsetting a watch-box with a snoring Leatherhead in it, or to lasso the sentry-box with a stout rope, and drag it along with its imprisoned occupant. But these experiences did not seriously ruffle the temper of the Watchmen, and so nobody was much the worse off for those irregular pleasantries.[62]

Incremental efforts, such as hiring full-time watch captains and detectives, and creating watch-houses and police courts, failed to secure public order.

Disorder in American cities was such that vigilance committees were set up in Philadelphia in 1849[63] and in New York City during the 1850s.[64] The antebellum cities of the North suffered race riots, nativist/Irish riots, riots between rival volunteer fire companies, and a steady stream of violent crime.[65] Whether, as a statistical matter, street crime had become worse than it had been in earlier decades is unknowable. As a matter of perception, there was something of a crisis mentality; and there was evidence to support the perception of crisis.[66]

---

[62] AUGUSTINE E. COSTELLO, OUR POLICE PROTECTORS 72-73 (Patterson Smith ed., 3d ed. 1972).

[63] *See* DAVID R. JOHNSON, POLICING THE URBAN UNDERWORLD: THE IMPACT OF CRIME ON THE DEVELOPMENT OF THE AMERICAN POLICE, 1800-1887, at 30-31 (1979).

[64] *See* MILLER, *supra* note 43, at 140.

[65] *See, e.g.*, SAMUEL WALKER, A CRITICAL HISTORY OF POLICE REFORM: THE EMERGENCE OF PROFESSIONALISM 4 (1977) (arguing that modern police forces were developed as a "consequence of an unprecedented wave of civil disorder that swept the nation between the 1830s and the 1870s").

[66] *See* ROBERT C. WADMAN & WILLIAM THOMAS ALLISON, TO PROTECT AND SERVE: A HISTORY OF POLICE IN AMERICA 30-31 (2004) (The year 1834 was remembered as "the year of the riots" in New York City; police reform followed the notorious unsolved murder of Mary Rogers in 1841.); JOHNSON, *supra* note 63, at 15 ("No reliable statistics survive in sufficient quantities to verify these charges, and the picture of a crime-ridden society was probably exaggerated. But the rhetoric indicates a widespread belief that crime had become a major problem, and in the absence of any contrary evidence, that attitude became an important justification for changing the existing law enforcement machinery." (footnote omitted)). The only skeptical challenge to the link between urban crime and the new police appears to be Professor Erik Monkkonen's view. *See* ERIK H. MONKKONEN, MURDER IN NEW YORK CITY 7 (2001) (challenging assumption of police as "natural" response to urban crime). Monkkonen's own account of police emerging as part of the service package provided by city governments, however, does not explain why some services including security services came to be provided primarily by urban government while other services remained private,

The first American police force, organized on the so-called "metropolitan model" of the London force, is usually said to be New York City's, organized initially in 1845.[67] Boston also claims this distinction based on an authorizing statute passed in 1837,[68] but in any event, full-time police forces quickly became standard in major cities: Philadelphia in 1855; Chicago, Pittsburgh, and San Francisco in 1857; Washington, D.C. in 1861; and Cleveland in 1866.[69] The new, professional, round-the-clock, paramilitary police forces also undertook the task of investigating suspected offenses, even in the absence of any complaint from the citizenry.

By 1886, the year of the so-called Haymarket Riot in Chicago, order was kept by full-time, round-the-clock professional police armed with repeating firearms. Offenses were investigated by police detectives working with a public prosecutor who possessed a practical monopoly on charging decisions. So when a bitter crowd of labor sympathizers massed to protest police brutality, they were met by a column of hundreds of armed officers in uniform and under the observation of informants and plainclothes detectives in their midst.[70] After the immediate violence of the Haymarket Riot ended, the police conducted a brutal investigation in which the police, without warrants, ransacked homes and newspaper offices.[71] Hundreds were arrested, interrogated by such means as

---

running the gamut from construction to the regulated utilities. And Monkkonen's own subsequent study of homicide in New York shows that New York was indeed a more violent place than London or Liverpool. *See id.* at 134-50. That at least suggests that there was a security challenge in nineteenth-century American cities.

[67] JAMES F. RICHARDSON, THE NEW YORK POLICE: COLONIAL TIMES TO 1901, at 49 (1970).

[68] ROGER LANE, POLICING THE CITY—BOSTON 1822-1825, at 37 (1967).

[69] These dates are drawn from ERIC H. MONKKONEN, POLICE IN URBAN AMERICA 164-68 (1981). Monkkonen used the date of the adoption of uniforms as a proxy for metropolitan departments of the modern type. *Id.*

[70] On the Haymarket affair, see generally PAUL AVRICH, THE HAYMARKET TRAGEDY (1986); and JAMES GREEN, DEATH IN THE HAYMARKET (2006).

[71] *See* AVRICH, *supra* note 70, at 221 ("Meeting halls, newspaper offices, and even private homes were invaded and ransacked for evidence. In two days more than fifty gathering places of anarchists and socialists were raided and persons under the slightest suspicion of radical affiliation arrested, in most cases without warrants and with no specific charge lodged against them . . . The next few weeks saw the detention of hundreds of men and women, most of them foreigners, who were put through the 'third degree' to extract information and confessions.").

the sweatbox.[72] A handful of leading anarchists were selected by the state's attorney to be presented to the grand jury for indictment and trial.[73]

In short: The 1791 criminal justice system was amateurish, reactive, and took little action absent judicial authorization. The modern system that emerged in the course of the nineteenth century was professional, proactive, and operated on an industrial scale, substantially without judicial oversight.

C. The Contextual Critique of SPO

The specific rules and practices regulating search and seizure in 1791 functioned in a system that otherwise vanished during the nineteenth century. To interpret the general language of the Fourth Amendment as instantiating the particular rules, after radical change to the system of which those rules were integral components, is *not* a faithful rendition of the original understanding. Simply put, any given 1791 search-and-seizure rule *is not the same rule* in a completely different criminal justice system.

I shall illustrate this claim with some specific examples. Following the helpful taxonomy developed by Professor Rubenfeld,[74] I divide these into two categories: founding-era application understandings and founding-era no-application understandings. An "application understanding" is an expectation that a constitutional provision prohibits some specific historical abuse. A "no-application understanding" is the expectation that the constitutional provision does not prohibit some rule or practice. Rubenfeld convincingly argues that in general "application understandings," especially those against the very practices that motivated the adoption of the constitutional provision, have proved more durable in our law than no-application understandings.[75] In the Fourth Amendment context, however, the Court has abandoned even core application understandings. The Court has done so for compelling reasons attending the revolutionary changes in the criminal justice system that took place in the century after the founding. Those changes not only mean that actual implementation of SPO would be bad, perhaps catastrophic, policy. The systemic changes also make SPO an illogical objection to what the Court has done.

---

[72] *Id.*

[73] The legal proceedings eventually reached the U.S. Supreme Court, which refused to overturn the convictions. *See Ex Parte* Spies, 123 U.S. 131, 163-66 (1887).

[74] *See* Jed Rubenfeld, *The Paradigm Case Method*, 115 YALE L.J. 1977 (2006).

[75] *See id.* at 1981 ("American constitutional law adheres systematically to one kind of original understanding (which I call 'foundational Application Understandings'),

1. Founding-Era Application Understandings

All agree that the Fourth Amendment was understood to ban general warrants and writs of assistance. General warrants, although widely used in both England and America, became objects of Whig outrage after royal officers arrested John Wilkes for criminal libel in 1763.[76] Wilkes had published a scurrilous, war-mongering pamphlet criticizing the government.[77] The government retaliated: "Upon an information for libel filed by the attorney-general, general search warrants were issued by one of the secretaries of state leading to the arrest of no less than forty-nine persons, including Wilkes, his printer, and his publisher."[78] "Every closet, bureau, and drawer in one Wilkes residence was opened in an effort to find and confiscate the entirety of his papers."[79] Hundreds of locks were broken and thousands of documents taken.[80]

Freed by a writ of habeas corpus, Wilkes fled abroad and was convicted of criminal libel *in absentia*.[81] Popular opinion was overwhelmingly on his side.[82] Wilkes returned to England to serve

---

while routinely discarding all other original understanding (which I call 'No-Application Understandings')."').

[76] For an overview of the Wilkes affair, see CLANCY, *supra* note 16, at 35-38 (2008).

[77] For the famous pamphlet, *The North Briton*, No. 45, see THE NORTH BRITON NO I TO NO. XLVI INCLUSIVE 157 (1769).

[78] LEONARD W. LEVY, LEGACY OF SUPPRESSION: FREEDOM OF SPEECH AND PRESS IN EARLY AMERICAN HISTORY 145 (1960).

[79] CUDDIHY, *supra* note 17, at 442.

[80] *Id.* ("Although unquestionably exaggerated, Wilkes' inventory of damages reflected outright plunder on a scale that neither the Huns, the Gestapo, nor the N.K.V.D. could have exceeded.").

[81] *See* LEVY, *supra* note 78, at 146.

[82] *See, e.g.*, JOHN BREWER, PARTY IDEOLOGY AND POPULAR POLITICS AT THE ACCESSION OF GEORGE III, at 178-79 (1976) (describing public demonstrations

his sentence and was elected to Parliament while in prison.[83] He and his associates brought tort actions against the officers who conducted the search.[84] The defendants could not deny that they had entered private premises and taken private property without consent.[85] That made them trespassers, unless they could point to some legal justification.

They claimed two such justifications. The first was a quasi-judicial immunity, based on the statutory immunity given to justices of the peace under the Vagrancy Act.[86] The second was the warrant issued by the secretary of state. The common-law courts of Common Pleas and King's Bench rejected both defenses.[87]

The controversy over writs of assistance arose from British efforts to raise revenue in the American colonies.[88] John Adams heard, and was inspired by, James Otis' famous argument against the writs in 1761.[89] Based on English practice, the Massachusetts Superior Court rejected Otis' arguments and upheld the legality of the writs.[90] The Massachusetts court granted at least ten writs in the next four years.[91] The colonial courts, however, generally refused to issue the writs or issued them in modified form.[92] John

---

celebrating release of Wilkes in 1770 and a 1769 petition on his behalf that was signed by 55,000).

[83] LEVY, *supra* note 78, at 146.

[84] There were dozens of suits. *See* CUDDIHY, *supra* note 17, at 439-68.

[85] For example, in *Entick v. Carrington*, 19 How. St. Tr. 1030 (C.P. 1765), the jury by special verdict found that the defendants had forcibly entered and would be trespassers if they did not have a justification. *Id.* at 1036.

[86] *See, e.g.*, *Entick*, 19 How. St. Tr. at 1039-41 (argument of defendant's counsel).

[87] The cases most commonly cited are: *Leach v. Money*, 97 Eng. Rep. 1050 (K.B. 1765); *Entick v. Carrington*, 95 Eng. Rep. 807 (C.P. 1765); *Huckle v. Money*, 95 Eng. Rep. 768 (C.P. 1763); and Wilkes v. Wood, 98 Eng. Rep. 489 (C.P. 1763). *Entick*, strictly speaking, did not involve the Wilkes warrant, but rather was brought by the publishers of another pamphlet, THE MONITOR, who had suffered arrest and search under an earlier general warrant. *See Entick,* 95 Eng. Rep. at 808.

[88] On the controversy generally, see M.H. SMITH, THE WRITS OF ASSISTANCE CASE (1978); and CUDDIHY, *supra* note 17, at 377-435, 489-536. For a sample of the writs in use in 1762, see WILLIAM MACDONALD, DOCUMENTARY SOURCEBOOK OF AMERICAN HISTORY 1606-1898, at 105-09 (1908).

[89] *See* 2 WORKS OF JOHN ADAMS 519-20 (1850).

[90] *See* CUDDIHY, *supra* note 17, at 394-95.

[91] *Id.*

[92] *Id.* at 530-36.

Adams would go on to draft Article 14 of the Massachusetts Declaration of Rights, the primary model for the Fourth Amendment.[93]

The central meaning of the Fourth Amendment is that general warrants and writs of assistance are prohibited. "Yet in the case of administrative searches, the Supreme Court has required officials to secure 'area warrants,' the modern analogue of general warrants, which are issued upon a showing that there is not individualized probable cause."[94] Is the "general warrant" for an administrative building inspection the same thing as the "general warrant" for promiscuous arrest and search issued against Wilkes? Or has government's need for proactive enforcement, coupled with the minimally coercive nature of administrative inspections, made today's "general warrants" not the same kind of "general warrants" the founders abhorred?

Inextricably connected to the ban on general warrants was the contemporaneous tort law, which made officers who entered private premises *without a particularized warrant* liable in damages. The Wilksite cases rejected any immunity for executive officers as such.[95] "Significantly, the defendants' argument did not go in terms of executive privilege or immunity."[96] A valid warrant defeated a trespass suit. An invalid warrant was the equivalent of no warrant at all, and without a good warrant, all trespassers, even public officers seeking in good faith to enforce the criminal law, were liable for both compensatory and punitive damages.[97]

As Professor Pfander puts it, "[T]he origins of qualified immunity have never been adequately explored or explained

---

[93] *See* Thomas K. Clancy, *The Framers' Intent: John Adams, his Era, and the Fourth Amendment*, 86 IND. L.J. 979, 1027-31 (2011).

[94] Louis Michael Seidman, *Acontextual Judicial Review*, 32 CARDOZO L. REV. 1143, 1147 (2011) (citing Camara v. Municipal Court, 387 U.S. 523 (1967) (holding that Fourth Amendment requires warrants for building inspections but warrants to inspect all buildings in a particular area are constitutional)).

[95] Louis L. Jaffe, *Suits Against Government and Officers: Sovereign Immunity*, 77 HARV. L. REV. 1, 16 (1963) (discussing Entick v. Carrington, 19 How. St. Tr. 1030 (C.P. 1765)).

[96] *Id.*

[97] On the exemplary damages awarded in the Wilksite cases, see CUDDIHY, *supra* note 17, at 452 (noting that Beardmore, another plaintiff against Carrington, received £1000).

. . . ."[98] It seems clear, however, that qualified immunity arose long after the founding. In *Little v. Barreme*, Chief Justice Marshall for a unanimous Court held that a navy captain who seized a vessel without statutory authority could not escape liability by proof of good-faith compliance with a presidential order.[99] Unfairness was mitigated by the congressional practice of passing private bills to indemnify sympathetic defendants.[100]

In *Wise v. Withers*, the plaintiff, a justice of the peace, sued the defendant, a collector of militia fines, for trespass after the collector entered the plaintiff's property and seized goods to satisfy a fine.[101] The plaintiff argued that as a justice of the peace he was exempt from militia service by act of Congress.[102] The Supreme Court, again per Chief Justice Marshall, agreed with the plaintiff that he was exempt from service. That being so, the order of a court marital imposing the fine gave the collector no defense: "[I]t is a principle, that a decision of such a tribunal, in a case clearly without its jurisdiction, cannot protect the officer who executes it. The court and the officer are all trespassers."[103] Absent a warrant, there was no public-officer immunity from suit.[104] Indeed, even when a warrant was erroneously issued by a court of competent jurisdiction, the officers were still exposed to liability.[105]

During Aaron Burr's trial for treason charges, the defense moved for an attachment of the person (i.e., an order to arrest) General Wilkinson for arresting witnesses who were to testify at the trial.[106] The defense theory was that these arrests, together with other misconduct by Wilkinson, amounted to a contempt of the trial court.[107] Chief Justice Marshall presided at the trial in the circuit court. Marshall rejected Burr's motion to have Wilkinson arrested because Wilkinson had acted under orders issued by Judge Hall.[108] Counsel for Burr argued that Hall was a puppet of Wilkinson's.[109]

---

[98] James E. Pfander, Iqbal, Bivens, *and the Role of Judge Made-Law in Constitutional Litigation*, 114 PENN. ST. L. REV. 1387, 1392 (2010) (footnote omitted).

[99] 6 U.S. 170, 179 (1804). To the same effect is *Otis v. Bacon*, 11 U.S. 589 (1813).

[100] *See generally* James E. Pfander & Jonathan L. Hunt, *Public Wrongs and Private Bills: Indemnification and Government Accountability in the Early Republic*, 85 N.Y.U. L. REV. 1862 (2010).

[101] 7 U.S. 331 (1806).

[102] *Id.* at 332.

[103] *Id.* at 337.

[104] *See* David P. Currie, *Sovereign Immunity and Suits Against Government Officers*, 1984 SUP. CT. REV. 149, 153 (1985); David E. Engdahl, *Immunity and Accountability for Positive Government Wrongs*, 44 U. COLO. L. REV. 1, 41-47 (1972); David L. Shapiro, *Wrong Turns: The Eleventh Amendment and the* Pennhurst *Case*, 98 HARV. L. REV. 61, 72 (1984).

[105] *See* Davies, *supra* note 17, at 649 (surveying early American cases, concluding: "[T]he common law apparently provided no justification for a search of a house beyond the ministerial execution of a valid search warrant." (footnote omitted)).

Marshall wrote as follows:

> Whether the judge did or did not transcend the limits prescribed by law, those ministerial officers who obeyed his orders cannot be supposed to have acted with a knowledge that he had mistaken his power. Should it be admitted that this would be no defence for them in an action to obtain compensation for the injury, yet it furnishes sufficient evidence that no contempt was intended to this court by General Wilkinson, that he has not been guilty of any intentional abuse of its process, or of any oppression in the manner of executing it.[110]

He goes on to say that:

> [W]here an attachment does not seem to be absolutely required by the justice due to the particular individual against whom the prosecution is depending, the court is more inclined to leave the parties to the ordinary course of law, than to employ the extraordinary powers which are given for the purpose of preserving the administration of justice in that purity which ought to be so universally desired.[111]

The upshot seems to be that if the witnesses sued Wilkinson for false arrest, even warrants, such as those issued by Judge Hall, would provide no good-faith defense if the court trying the tort action concluded that the warrants were issued erroneously.

---

[106] United States v. Burr, 25 F. Cas. 41, 49 (C.C.D. Va. 1807) (14,692f).

[107] *Id.*

[108] *Id.* at 48-49.

[109] *Id.* at 47.

[110] United States v. Burr, 25 F. Cas. 41, 49 (C.C.D. Va. 1807) (14,692f).

[111] *Id.*

Pierson v. Ray[112] and *Anderson v. Creighton*,[113] the Court's decisions recognizing qualified immunity for law enforcement officers in actions, brought, respectively, under 42 U.S.C. § 1983 and *Bivens*,[114] are bereft of founding-era support. So too are the various statutes and state court rulings recognizing "public function" qualified immunity against state tort claims.[115] If we want to restore the tort regime the founders expected, we would need to return to the practice of holding officers strictly liable for entries on a bad warrant or without any warrant at all.

Is that what the founders would have hoped for if they knew that the criminal law would come to be enforced by full-time, professional, proactive police? Professional police change the consequences of strict liability. Constables and watchmen served episodically and often reluctantly. Full-time police need to be recruited and retained, and they care about remaining in good standing with their employers. They have incentives to comply with legal standards apart from the fear of liability; and fear of liability might discourage people from taking jobs in law enforcement and undue passivity by those who serve.

The last two points could be addressed by indemnification, but only at high cost to the public fisc. The scope and intrusiveness of modern policing, relative to eighteenth-century law enforcement, raised the potential cost of indemnification dramatically. Immunity has the effect of leaving the costs of constitutional violations on the aggrieved citizen, thereby holding down the public expenditures for a given level of law enforcement. This may be good or bad policy (I am inclined to think it is bad),[116] but it is not a choice the founders could have harbored clear expectations about. At any rate, the *Houghton* formulation of SPO seems to call for the abolition of qualified immunity.

---

[112] 386 U.S. 547 (1967).

[113] 483 U.S. 635 (1987).

[114] *Bivens v. Six Unknown Named Agents*, 403 U.S. 388 (1971).

[115] *See, e.g.*, OHIO REV. CODE ANN. § 2744.03(A)(6) (LexisNexis 2003). The statute creates tort immunity for an employee of a political subdivision unless:

> (a) The employee's acts or omissions were manifestly outside the scope of the employee's employment or official responsibilities;
>
> (b) The employee's acts or omissions were with malicious purpose, in bad faith, or in a wanton or reckless manner;
>
> (c) Civil liability is expressly imposed upon the employee by a section of the Revised Code. Civil liability shall not be construed to exist under another section of the Revised Code merely because that section imposes a responsibility or mandatory duty upon an employee, because that section provides for a criminal penalty, because of a general authorization in that section that an employee may sue and be sued, or because the section uses the term 'shall' in a provision pertaining to an employee.

Id.

If we accept the historical account given in *Boyd v. United States*,[117] the founders had a distinct application understanding that the Fourth Amendment prohibited the seizure of private papers for evidentiary use. The *Boyd* Court relied on the Wilkes affair, and in particular Lord Camden's opinion in *Entick v. Carrington*, to condemn the seizure of papers. In *Entick*, Camden proclaimed:

> Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect. Where is the written law that gives any magistrate such a power? I can safely answer, there is none; and therefore it is too much for us without such authority to pronounce a practice legal, which would be subversive of all the comforts of society.[118]

---

[116] *See* Donald A. Dripps, *The "New" Exclusionary Rule Debate: From "Still Preoccupied with 1985" to "Virtual Deterrence,"* 37 FORDHAM URB. L.J. 733, 780 (2010) ("Given the prevalence of indemnification of individual officers, and the Supreme Court's extensive recognition of bright-line rules, tort liability sans immunity and sans exclusion might move us closer to optimal deterrence."). If we think that jury verdicts give a good estimate of the costs of Fourth Amendment violations, immunity, as compared to indemnification, amounts to subsidizing constitutional violations—leaving aside the officer-defendant's right to interlocutory appeal of an order denying immunity, which has a tendency to discourage even meritorious claims by increasing litigation costs.

[117] 116 U.S. 616 (1886).

[118] Entick v. Carrington, 19 How. St. Tr. 1030, 1066 (1765).

Boyd concluded that the founders embraced Camden's judgment and so meant to proscribe any seizure of private papers for evidentiary use against their owner.[119]

The *Boyd* Court's historical account deserves somewhat unusual deference, for two reasons. First, the opinion was written less than a century after the ratification of the Fourth Amendment. The justices had walked the earth with the founders.[120] If the passage of time makes the original understanding more difficult to recover, the *Boyd* Court has an advantage over us of more than a century.

Second, one of the members of the *Boyd* majority was Horace Gray, a legal historian. Significantly, he compiled the first archive of primary sources related to the Writs of Assistance controversy.[121] "Here, in almost 145 pages, packed with footnotes, Gray delivered a magnificent display of research into the origin and use of search warrants up to and at the time of Otis' arguments."[122] That archive remains "essential reading."[123] True, Gray was not an originalist.[124] But if Bradley's opinion had declared false history we would expect a deep student of the controversy over the writs, intimate with the grandson of John Adams,[125] to have known it and said something about it. In my view, the burden of proof is on those who assert that *Boyd* was wrong.

According to *Boyd*, the act struck down in that case:

---

[119] *Boyd*, 116 U.S. at 630.

[120] Justice Bradley was born in 1813. JOSEPH P. BRADLEY, MISCELLANEOUS WRITINGS (Charles Bradley ed., 1902). Thomas Jefferson and John Adams famously expired on or about the Fourth of July, 1826. JEAN EDWARD SMITH, JOHN MARSHALL: DEFINER OF A NATION 20 (1st ed. 1996). John Marshall lived until 1835. *Id.*

[121] Horace Gray, *Notes*, *in* REPORTS OF CASES ARGUED AND ADJUDGED IN THE SUPERIOR COURT OF JUDICATURE OF THE PROVINCE OF MASSACHUSETTS BAY BETWEEN 1761 AND 1772, at 395 (Boston, Little, Brown, & Co. 1865).

[122] Robert M. Spector, *Historian on the Supreme Court: Justice Horace C. Gray, Jr. and the Historical Method,* 12 AM. J. LEGAL HIST. 181, 194 (1968).

[123] Thomas K. Clancy, *The Role of History*, 7 OHIO ST. J. CRIM. L. 811, 812 (2010).

[124] Spector, *supra* note 122, at 209 ("Gray viewed the Federal Constitution as a living organism that meant one thing in 1789, an-other in 1860, and still another in his own time.").

[125] *Id.* at 209 (noting that Charles Francis Adams spent "many years of friendship" with Gray, although it appears that Adams thought Gray an unimaginative judge).

> was the first act in this country, and we might say, either in this country or in England, so far as we have been able to ascertain, which authorized the search and seizure of a man's private papers, or the compulsory production of them, for the purpose of using them in evidence against him in a criminal case, or in a proceeding to enforce the forfeiture of his property.[126]

Proving a negative is difficult, but I have not seen anything that would contradict the *Boyd* Court's assertion.

Professor Davies regards *Boyd*'s reliance on Camden's opinion in Howard's State Trials as erroneous. Davies argues that:

> Bradley's originalist claim was unsound because the passage he quoted had not appeared in the initial report of the 1765 case which was published in 1770 (with which many framing-era Americans undoubtedly were familiar), but appeared only in a later expanded case report that was not published until 1781. Thus, Americans could not have been familiar with the assertions that Bradley quoted when John Adams introduced the phrase "unreasonable searches and seizures" in the 1780 Massachusetts provision. Moreover, because it is unlikely that the later report would have been imported in significant numbers during the remainder of the framing era, it seems highly doubtful Americans would have become familiar with Camden's notion that a search warrant for papers was inherently illegal even by the time of the framing of the Fourth Amendment in 1789.[127]

At least with respect to private papers, *Boyd* is defensible against these objections.

On an "original public meaning" version of originalism, the question is not what was expected by Adams in 1780, but by

---

[126] Boyd v. United States, 116 U.S. 616, 622-23 (1886).

[127] *See* Thomas Y. Davies, *Can You Handle the Truth? The Framers Preserved Common Law Criminal Arrest and Search Rules in "Due Process of Law"—"Fourth Amendment Reasonableness" is Only a Modern, Destructive, Judicial Myth*, 43 TEX. TECH L. REV. 51, 117-18 (2010) (footnotes omitted).

Congress and the people in 1791[128]—by which time the expanded version of the report was in circulation.[129] Moreover, even Wilson's 1775 report says that "we can safely say there is no law in this country to justify the defendants in what they have done ; if there was, it would destroy all the comforts of society ; for papers are often the dearest property a man can have."[130]

In the pamphlet wars in the 1760s, Whig polemicists identified the seizure of papers as an abuse distinct from general warrants.[131] At the popular end of the spectrum, the anonymous *Brittania's Intercesion for the Deliverance of John Wilkes* declared, in mock-biblical rhetoric: "And they looked into his dwelling, and searched for his papers, and all his secret workings, and they took them every one."[132] The more cerebral "Father of Candor" laid out the same doctrine announced in *Boyd*: the seizure of papers was an "absolute illegality," an "abominable outrage,"[133] and the use of seized papers at a criminal trial "would be making a man give evidence against and accuse himself, with a vengeance."[134] The letter further stated:

---

[128] *See, e.g.*, Kurt T. Lash, *The Origins of the Privileges or Immunities Clause, Part II: John Bingham and the Second Draft of the Fourteenth Amendment*, 99 GEO. L.J. 329, 338-39 (2011) ("Today, most originalist scholars reject original intent originalism and instead seek evidence of original public understanding. This approach seeks to determine the likely public understanding of a proposed constitutional text, with special emphasis placed on those with the authority to ratify the text and make it an official part of the Constitution." (footnotes omitted)).

[129] *See* Roger Root, *The Originalist Case for the Fourth Amendment Exclusionary Rule*, 45 GONZ. L. REV. 1, 41-42 n.260 (2009-2010) ("Moreover, the set of books containing the longer version (Hargrave's *A Complete Collection of State-Trials and Proceedings For High-Treason, and other Crimes and Misdemeanours* (known as *State Trials*, 4th edition (1781))[)] was a fixture of late-eighteenth-century law libraries. Over a hundred of these sets survive in the rare book collections of American libraries today, and several libraries (e.g., Yale's and Harvard's) hold more than one complete set. The notion that all of these book sets, published in 1781, crossed the Atlantic only after the Fourth Amendment was proposed and ratified (between September 1787 and December 1791) seems highly unlikely.").

[130] Entick v. Carrington, 95 Eng. Rep. 807, 817-18 (C.P. 1765).

[131] *See* Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869, 896-907 (1985); CUDDIHY, *supra* note 17, at 459-60 (1990).

[132] BRITTANIA'S INTERCESSION FOR THE DELIVERANCE OF JOHN WILKES, ESQ. FROM PERSECUTION AND BANISHMENT TO WHICH IS ADDED, A POLITICAL AND CONSTITUTIONAL SERMON: AND A DEDICATION TO L— B—, at 7 (London, H. Woodgate 1768).

[133] A LETTER CONCERNING LIBELS, WARRANTS, THE SEIZURE OF PAPERS AND SURETIES FOR THE PEACE OF BEHAVIOUR; WITH A VIEW TO SOME LATE PROCEEDINGS, AND THE DEFENCE OF THEM BY THE MAJORITY 54 (London, J. Almon 5th ed. 1765), *available at* http://books.google.com/books?id=aVICAAAAMAAJ&pg=PA4&dq=candor+letter+concerning+libels&hl=en&ei=ns8kTunjNtDAgQf_4W7DA&sa=X&oi=book_result&ct=result&resnum=1&ved=0CCkQ6AEwAA#v=onepage&q&f=false.

> It must either be sworn that I have certain stolen goods, or such a particular thing that is criminal itself, in my custody, before any magistrate is authorized to grant a warrant to any man to enter my house and seize it. Nay further, if a positive oath be made, and such a particular warrant issued, it can only be executed upon the paper or thing sworn to and specified, and in the presence of owner or of somebody intrusted by him, with the custody of it.[135]

American patriots revered Wilkes and paid close attention to his tribulations.[136]

Davies further argues that the text of the Fourth Amendment implicitly authorizes searches of "papers."[137] The reasonableness clause lists the interests protected by the right against unreasonable searches in descending order of priority: persons, houses, paper, then effects. Why mention papers at all? If "things" in the warrant clause is synonymous with "effects" in the reasonableness clause, then indeed the warrant clause implies that papers are not among the "things to be seized" even by valid warrant. If we equate "things" in the warrant clause with "effects" in the reasonableness clause, the text arguably cuts in exactly the other directions. "Things" can be seized, but papers are not like other "things" or other "effects."

In any event, even under *Entick* and *Boyd* there could be reasonable seizures of papers: stolen papers or contraband papers such as libels and (later) lottery tickets. The constitutional status of the ban on warrants to search for and seize documentary evidence was recognized, long before *Boyd,* by the Massachusetts court in *Commonwealth v. Dana*, decided in 1841.[138] Dana was convicted of possessing materials for a lottery, and moved in arrest of judgment on the ground, *inter alia*, that the papers used against him as evidence were obtained by the execution of an unconstitutional warrant.[139] Justice Wilde gave two grounds for rejecting Dana's position. The first was the lottery materials, once banned by the legislature, became subject to seizure like libels or stolen goods.[140] The second was that even if the warrant was illegal, Dana's remedy was to sue for trespass, not to exclude the evidence.[141]

---

[134] *Id.* at 55-56.

[135] *Id.* at 58.

[136] *See* BERNARD BAILYN, THE IDEOLOGICAL ORIGINS OF THE AMERICAN REVOLUTION 110-12 (Harvard Univ. Press 1967); Pauline Maier, *John Wilkes and American Disillusionment with Britain*, 20 WM. & MARY Q. 373 (1963).

[137] *See* Davies, *supra* note 127, at 118-19.

[138] 43 Mass. (2 Met.) 329 (1841).

On the second point *Dana* differs from *Boyd*, but not on the first. The *Dana* court quoted approvingly the "dearest property" language from *Entick*. The *Dana* opinion takes pains to note that the only papers seized were contraband, not mere evidence:

> It has been objected further, that the warrant was illegally served, because the officer seized "books, &c.," and it is argued that books are not ""materials for a lottery." But we think that books, kept in relation to the proceedings respecting a lottery, are to be considered as materials for a lottery; and it does not appear that any other books were seized.[142]

The amendment does not speak to seizing any property, let alone "papers," for use in evidence without the right to confiscate them. While further investigation is justified, the evidence so far suggests that the original public meaning of the Fourth Amendment included a special hostility to seizing private papers.

Would that understanding have withstood prescient awareness of our government's need to combat fraud and terrorism in a computer age? That seems beyond any certain knowledge but on the whole unlikely. I suppose one might stretch the concept of "instrumentalities" of crime to cover far more documentary (or conversational) evidence than might be supposed at first blush.[143] It would be stretched to the breaking point if that notion went so far as to include Ted Kaczynski's diary or every file stored on Zacarias Moussaoui's computer.

---

[139] *Id.* at 331-32.

[140] *Id.* at 337.

[141] *Id.*

[142] *Id.* at 337.

Terry stops provide a fourth example of the irrationality of privileging specific application understandings. Blackstone states:

> To constitute the injury of false imprisonment there are two points requisite : 1. The detention of the person ; and, 2. The unlawfulness of such detention. Every confinement of the person is an imprisonment, whether it be in a common prison, or in a private house, or in the stocks, or even by forcibly detaining one in the public streets. Unlawful, or false, imprisonment consists in such confinement or detention without sufficient authority : which authority may arise either from some process from the courts of justice ; or from some warrant from a legal officer having power to commit, under his hand and seal, and expressing the cause of such commitment; or from some other special cause warranted, for the necessity of the thing, either by common law, or act of parliament ; such as the arresting of a felon by a private person without warrant, the impressing of mariners for the public service, or the apprehending of waggoners for misbehaviour in the public service, or the apprehending of waggoners for misbehaviour in the public highways.[144]

The founders, then, would have expected the legality of a so-called *Terry* stop to be tested by an action for false imprisonment. If we characterize a *Terry* stop as forcible detention based on suspicion falling short of probable cause, these stops would have been actionable according to founding-era common law. Indeed, founding-era warrantless arrest standards were actually stricter than the modern probable cause formulation.[145]

---

[143] Justice Brennan wrote, when *Boyd* was still good law, "that words, which are the objects of an electronic seizure, are ordinarily mere evidence and not the fruits or instrumentalities of crime, and so they are impermissible objects of lawful searches under any circumstances." Lopez v. United States, 373 U.S. 427, 462 (1963) (Brennan, J., dissenting). On the other hand, Justice Sutherland noted an important distinction in a memo he wrote while *Olmstead* was being decided. "In a general way my view is that the conversations which were heard as a result of the wire tapping did not relate to a past crime but were part of a crime then being committed." *See* Robert Post, *Federalism, Positive Law, and the Emergence of the American Administrative State: Prohibition in the Taft Court Era*, 48 WM. & MARY L. REV. 1, 146 (2006). Sutherland denied that wiretapping was a search or a seizure, but assuming it were, Sutherland's point that forward-looking co-conspirator statements would be instrumentalities and so seizable under *Boyd* is perfectly logical.

[144] 3 WILLIAM BLACKSTONE, COMMENTARIES *127 (footnotes omitted).

But to abstract the false imprisonment tort from the legal context would be misleading. At the founding, justices of the peace had statutory authority to try summarily, and punish corporally, offenses "such as common swearing, drunkenness, vagrancy, idleness, and a vast variety of others[.]"[146] The practice was common enough that one cost of these summary proceedings was that the press of cases made some unwilling to serve as a justice.[147]

In the nineteenth century, the new police forces were given some broader arrest powers than enjoyed by private persons.[148] Their principal security against liability for false arrest or false imprisonment, however, appears to have been that the substantive law made suspicious public behavior of the sort, now dealt with under *Terry*, criminal. Between 1845 and 1850, the New York Police Department recorded 144,364 arrests.[149] Of these, 20,252 were for "Disorderly conduct," 29,190 for "Intoxication and disorderly conduct," 36,675 for "Intoxication" simpliciter, and 11,347 for "Vagrancy."[150] Another 733 were for "Assault and interfering with Policeman."[151]

In form, statutory provisions such as "vagrancy" and "disorderly conduct" define substantive offenses. In practice, they authorize arrest and search for suspicious behavior. A statute that made it a crime to refuse consent to search, or to "engage in conduct that would cause a reasonably prudent person to believe that criminal activity may be afoot" would, I suppose, violate the Fourth Amendment. But vagrancy-type offenses were not struck down as void-for-vagueness on due-process grounds until the 1960s and 1970s.[152]

---

[145] *See* Davies, *supra* note 17, at 627-34 (founding-era common-law authorized warrantless arrest if the officer (or private citizen) actually saw an offense; if the arrested suspect was indeed guilty of a felony as established by his subsequent conviction; or when a felony was in fact committed and the officer had reasonable grounds for suspecting the person arrested of committing it).

[146] BLACKSTONE, *supra* note 39, at *278.

[147] *Id.* at *279.

[148] *See* Davies, *supra* note 17, at 634-42.

[149] COSTELLO, *supra* note 62, at 116.

[150] *Id.*

[151] *Id.*

Would the Framers have condemned *Terry* stops if they knew that the prohibition of vagrancy would be invalidated, and that police would be on proactive patrol at all hours? Perhaps they would have, but the utterly changed legal and institutional context makes such a judgment highly speculative.

Consider one more founding-era application understanding. William Cuddihy asserts that second only "to the requirement for specificity in warrants, the hidden unconstitutionality of nocturnal searches was the most certain feature of the amendment's original understanding."[153] The terrors of night-time home invasion, however, while not eliminated, are certainly dramatically reduced by electric light, telephone communications, and uniformed police. A "nighttime entry" in 1791 was a different experience than a "nighttime entry" in 2011.

In sum, on many points the founders probably regarded many specific modern practices to be "unreasonable." These include warrantless entries for regulatory purposes, qualified immunity for police officers, warrants to search for and seize private papers as evidence, and *Terry* stops based on less than probable cause. It is far from clear, however, that these specific expectations should be regarded as controlling given the massive institutional changes in the criminal justice system since the founding.

Today we tolerate building inspections under general warrants, qualified immunity for warrantless police actions, and the routine seizure of papers for use in evidence. We do this because in the changed institutional context of modern, proactive law enforcement, we see nothing "unreasonable" in these particular practices. The founders saw them as prototypically unreasonable, but only in an institutional context so removed from ours that we cannot say their original expectations would have survived changed circumstances.

---

[152] *See* Papachristou v. City of Jacksonville, 405 U.S. 156 (1972); Shuttlesworth v. City of Birmingham, 382 U.S. 87 (1965).

[153] CUDDIHY, *supra* note 17, at 1510.

2. Founding-Era No-Application Understandings

Just as the founders aimed to prohibit specific practices we now tolerate, they also tolerated some practices that we now forbid. The most frequently mentioned example is eavesdropping, which absent a trespass required no warrant at common law. *Katz* is usually seen as a response to technological change. Institutional changes, however, were a major impetus toward regulating electronic surveillance.

In the founding era, eavesdroppers were private sneaks. Their snooping, even if not actionable under tort law, was a petty criminal offense.[154] The usual, and indeed powerful, reason given for expanding the Fourth Amendment to cover *electronic* surveillance is technological change.[155] Technology, however, is only half the story. Our intuitions about eavesdropping vary not only with the technology used, but also with the identity of the people using the technology. Consider private eavesdropping.[156] It is hard to think of a justification for *private* eavesdropping. Nor, at least until the internet age, was it plausible to think of private eavesdropping as offering private persons a surplus of benefits over costs that would threaten general confidence in conversations behind closed doors or over the telephone.

Eavesdropping *by government agents* is in another category altogether. Justice Black was right in *Katz* that the founders knew about eavesdropping.[157] I disagree, as did *Katz* and all subsequent cases, with Justice Black's further claim that "wiretapping is nothing more than eavesdropping by telephone."[158] Leaving the technological aspect aside, Justice Black was wrong about something else. The Framers were as ignorant of eavesdropping by proactive professional law-enforcement agents as they were of wiretapping.

---

[154] BLACKSTONE, *supra* note 39, at *169 ("Eaves-droppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nusance and presentable at the court-leet: or are indictable at the sessions, and punishable by fine and finding sureties for the good behavior.").

[155] *See, e.g.*, United States v. White, 401 U.S. 745, 755 (1971) (Douglas, J., dissenting) ("What the ancients knew as 'eavesdropping,' we now call 'electronic surveillance'; but to equate the two is to treat man's first gunpowder on the same level as the nuclear bomb.").

[156] *See, e.g.*, Don Van Natta Jr., *Suspicions about Former Editor in Battle over Story Complicate Hacking Scandal*, N.Y. TIMES, July 23, 2011 at A4 (eavesdropping allegedly used by employees of the tabloid press).

It is at least arguable that institutional changes had more influence than technological ones on the Court's turn in *Katz.* Proactive enforcement transformed eavesdropping, by whatever means, from an eccentric private vice to a pervasive public threat. This transformation manifested itself in police spying on labor unions[159] and ferreting out homosexual liaisons.[160] Surely, however, the most salient fact about electronic surveillance *by police* was its troubling similarity to the practices of Nazi Germany and Soviet Russia.[161]

The term "police state" appears for the first time in a Supreme Court report in 1947. Dissenting from a holding premised on a broad view of the warrantless search power incident to lawful arrest, Justice Frankfurter declared: "The whole point about the Fourth Amendment is that 'Its protection extends to offenders as well as to the law abiding,' because of its important bearing in maintaining a free society and avoiding the dangers of a police state."[162] Freshly returned from prosecuting the leading Nazis, Justice Jackson separately dissented, and admitted that requiring warrants might shelter the guilty.[163] "But the forefathers thought this was not too great a price to pay for that decent privacy of home, papers and effects which is indispensable to individual dignity and self-respect."[164] Indeed, a distinct streak of "anti-totalitarianism" ran through the Warren Court's criminal procedure revolution.[165]

---

[157] Katz v. United States, 389 U.S. 347, 366 (1967) ("Tapping telephone wires, of course, was an unknown possibility at the time the Fourth Amendment was adopted. But eavesdropping (and wiretapping is nothing more than eavesdropping by telephone) was, as even the majority opinion in Berger, *supra*, recognized, an ancient practice which at common law was condemned as a nuisance." (citations omitted) (internal quotation marks omitted)).

[158] *Id.*

[159] *See, e.g.*, Wesley M. Oliver, *The Neglected History of Criminal Procedure, 1850-1940*, 62 RUTGERS L. REV. 447, 521-22 (2010) (describing labor support for limits on wiretapping, backed by an exclusionary rule, in 1938 at the New York constitutional convention).

[160] *See* David Alan Sklansky, *"One Train may Hide Another":* Katz, *Stonewall, and the Secret Subtext of Criminal Procedure*, 41 U.C. DAVIS L. REV. 875, 879 (2008) ("[T]he conception of privacy championed in Katz resonated strongly with the concerns raised by toilet stall spying, and by the harassment of gay men and lesbians more broadly.").

[161] *See, e.g.*, *White*, 401 U.S. at 760 (electronic surveillance "uncontrolled, promises to lead us into a police state") (Douglas, J., dissenting).

What revulsion at totalitarian police practices, revulsion at political uses of police surveillance, and revulsion at police harassment of homosexuals have in common is so obvious we might miss it: police. Without professional proactive police, none of these concerns would be relevant to American law enforcement. The founders, as we have seen, knew constables and the night watch. To investigate their understanding of the Fourth Amendment in an institutional world where law enforcement power is used, and abused, by the modern police is at least as nonsensical as investigating the founders' views of modern surveillance technology.

A less salient, but perhaps still clearer, example of how institutional changes have altered the presuppositions of founding-era no-application expectations is the use of deadly force to apprehend fleeing felons. In *Tennessee v. Garner*, the Supreme Court held that police violate the Fourth Amendment when they shoot a fleeing felony suspect unless the suspected offense, or the fugitive's conduct, supports an inference that the fugitive poses a potentially deadly threat.[166] The common-law rule clearly was to the contrary; deadly force could be used to apprehend any fleeing felon.[167] The *Garner* court openly repudiated the common-law rule,[168] emphasizing that the rule had originated when felonies were capital and when weaponry was crude.[169]

---

[162] Harris v. United States, 331 U.S. 135, 171 (1947) (Frankfurter, J., dissenting) (citation omitted).

[163] *See* Carol Steiker, *Second Thoughts about First Principles*, 107 HARV. L. REV. 820, 842 (1994) ("During the trial of 1945 to 1946, Justice Jackson gathered and presented evidence of the systematic use of Nazi police power to commit genocide—the most extreme and racially discriminatory use of law enforcement institutions the world had ever witnessed. Justice Jackson returned to the Supreme Court a fervent believer in the warrant requirement.").

[164] *Harris*, 331 U.S. at 198 (Jackson, J., dissenting).

[165] *See* Richard Primus, *A Brooding Omnipresence: Totalitarianism in Postwar Constitutional Thoughts*, 106 YALE L.J. 423, 444-45 (1996) (noting how opinions in *Gideon* and *Escobedo* exploited the contrast with Soviet show-trials); Margaret Raymond, *Rejecting Totalitarianism: Translating the Guarantees of Criminal Procedure*, 76 N.C. L. REV. 1193, 1197 (1998).

The point that at the founding-era felonies were capital, although often made, seems far less forceful than one might suppose. On paper, the felonies were capital but after jury nullification, judicial scrutiny of the indictment on a motion in arrest, benefit of clergy, and application for a pardon, the chance that any given suspected felon would actually hang was very small. Recall that in 1791 only one person in America is known to have been executed for burglary.[170] The limited accuracy of founding-era firearms may have meant that deadly force would usually be resorted to only in hand to hand combat, but the common-law rule was articulated as a special one for apprehending fleeing felons, not a proxy for when self-defense principles would provide a defense.[171]

The far more convincing explanation is that the inefficiency of the eighteenth-century system put a high premium on apprehending offenders *in flagrante*. Court records were kept, but not police records (there were no police); communications were slow (even the telegraph was not yet invented); and identification utterly primitive (Alphonse Bertillon, the father of modern identification science, was not born until 1853).[172] Today there is a good chance of eventually making the case against the suspect even if he wins a footrace with arresting officers.

---

[166] Tennessee v. Garner, 471 U.S. 1 (1985).

[167] *Id.* at 11-12.

[168] *See id.* at 13 ("Because of sweeping change in the legal and technological context, reliance on the common-law rule in this case would be a mistaken literalism that ignores the purposes of a historical inquiry.").

[169] *Id.* at 14-15.

[170] *See Executions in the United States, 1608-2002: The ESPY File*, DEATH PENALTY INFORMATION CENTER *available at* http://www.deathpenaltyinfo.org/documents/ESPYyear.pdf.

[171] *See* MICHAEL FOSTER, A REPORT OF SOME PROCEEDINGS ON THE COMMISSION FOR THE TRIAL OF THE REBELS IN THE YEAR 1742, IN THE COUNTY OF SURRY; AND OF OTHER CROWN CASES: TO WHICH ARE ADDED DISCOURSES UPON A FEW BRANCHES OF THE CROWN LAW 272 (London, E. & R. Brooke 3rd ed. 1809). Foster clearly distinguished the privilege to use deadly force to apprehend felons from the *se defendo* plea, pointed out that the execution of all felons was "a presumption against fact," and rested the law-enforcement privilege on the public safety. *Id.*

The basic point is that specific founding-era no-application expectations can be just as misleading as application understandings. Rules that made sense for a reactive amateur system may make no sense for a professional proactive system, and it is arbitrary to suppose that the founders would have clung to specific rules when a changed institutional context made those rules dysfunctional. In the words of Professor Davies, "Applying the original meaning of the language of the Fourth Amendment in a completely changed social and institutional context would subvert the purpose the Framers had in mind when they adopted the text."[173] In any event, if there is a principled approach to interpreting the Fourth Amendment other than SPO, the various unpalatable outcomes SPO points toward are good reasons indeed for embracing that alternative.

III. THE DYNAMISM CRITIQUE

Joseph Story wrote that the Fourth Amendment "is little more than the affirmance of a great constitutional doctrine of the common law."[174] The Framers, however, knew that common-law doctrine could change. Rules of the common law could be changed judicially, when the judges decided to overrule precedent or to follow one authority rather than another in conflict with the first. Common-law rules could also be changed by the legislature when it adopted statutes to supersede them. Let us consider the implications of a constitutional provision affirming common-law doctrine with respect to each avenue of common-law dynamism.

---

[172] *Alphonse Bertillon (1853-1914),* SCIENCEMUSEUM, http://www.sciencemuseum.org. uk/broughttolife/people/alphonebertillon.aspx (last visited Feb. 22, 2012).

[173] Davies, *supra* note 17, 740-41.

[174] JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES 709 (Boston, Hilliard, Gray & Co. 1833).

A. Judicial Changes in Common-Law Doctrine

The founders expected courts to observe the rule of stare decisis.[175] They did not, however, believe that precedents were never to be overruled. Blackstone wrote that precedents controlled but not when "flatly absurd or unjust."[176] Blackstone's view of precedent was more rigorous than Chancellor Kent's, who wrote in 1826:

> But I wish not to be understood to press too strongly the doctrine of stare decisis, when I recollect that there are one thousand cases to be pointed out in the English and American books of reports, which have been overruled, doubted, or limited in their application. It is probable that the records of many of the courts in this country are replete with hasty and crude decisions; and such cases ought to [be] examined without fear, and revised without reluctance, rather than to have the character of our law impaired, and the beauty and harmony of the system destroyed by the perpetuity of error. Even a series of decisions are not always conclusive evidence of what is law; and the revision of a decision very often resolves itself into a mere question of expediency, depending upon the consideration of the importance of certainty in the rule, and the extent of property to be affected by a change of it.[177]

While the founders, like jurists today, had views on just *how strong* a reason is required for overruling precedent, they seem to have had views on overruling not very different from those that can be found today.[178]

---

[175] For an extensive survey, see John O. McGinnis & Michael B. Rappaport, *Reconciling Originalism and Precedent*, 103 NW. U. L. REV. 803, 823 (2009) ("Precedent was supported by the leading founders of the country, including James Madison, Alexander Hamilton, Thomas Jefferson, James Wilson, and John Adams, as well as by leading legal giants, including Coke, Hale, Blackstone, and Kent. This is a veritable who's who of Founders and legal giants.").

[176] 1 WILLIAM BLACKSTONE, COMMENTARIES *70.

[177] JAMES KENT, 1 COMMENTARIES ON AMERICAN LAW 477 (New York, O. Halsted 1826).

[178] *See, e.g.*, Richard W. Murphy, 78 NOTRE DAME L. REV. 1075, 1089-90 (2003) ("[G]enerally speaking, they embraced the view that precedents should be treated as

There is a large body of literature addressing the question of whether a decision giving the Constitution an erroneous interpretation deserves continued fidelity.[179] The question here is quite different. It is to what extent a constitutional provision affirming a common-law doctrine freezes that doctrine as it stood upon ratification, or instead affirms that doctrine as it might evolve under a flexible rule of stare decisis.

To take a concrete example, think of the warrant for stolen goods. At common law, as stated in *Entick*, it had to be based on the citizen's oath that the goods were stolen, "strong reason" to believe the goods to be at a specific place, and "if the goods are not found *there,* he [the complainant] is a trespasser" and the officer is a witness to the trespass.[180] The rule in customs searches was different; the officers were not liable if the warrant was valid but the goods not found.[181] But it was not until the 1831 New York case of *Beaty v. Perkins*[182] that an American court rejected the common-law rule about stolen goods in trespass cases.

If SOP is right, *Beaty* is wrong. Leaving aside the unpalatable nature of that result, this seems to neglect the flexible view of stare decisis held by the Framers. If what the Fourth Amendment did was affirm "a great constitutional doctrine of the common law,"[183] it affirmed that doctrine in the dynamic form the founders knew characterized all common-law doctrines.

The risk of indeterminacy poses the obvious dilemma. Could modern courts approve general warrants or writs of assistance?

---

evidence of law that should be followed absent a demonstrably good reason to reject them.") (surveying views of Blackstone, Kent, Cranch, Swift, Wilson and Marshall).

[179] For an overview, see David L. Shapiro, *The Role of Precedent in Constitutional Adjudication: An Introspection*, 86 TEX. L. REV. 929, 930-40 (2008).

[180] Entick v. Carrington, 95 Eng. Rep. 807, 818 (C.P. 1765). There is a debate about whether liability was cut off automatically if the suspected goods were found. *Compare* Davies, *supra* note 17, at 647-48, *with* Fabio Arcila, Jr., *The Death of Suspicion*, 51 WM. & MARY L. REV. 1275, 1316-24 (2010). *Entick* seems clear that liability was automatic in the reverse situation; and Hale had stated the same view. *See* Davies, *supra* note 17, at 653 n.293.

[181] Cooper v. Boot, 4 Dougl. 338, 348-49, 99 Eng. Rep. 911, 916 (K.B. 1785).

[182] Beaty v. Perkins, 6 Wend. 382 (N.Y. Sup. Ct. 1831). *Beaty* was questioned in *Chipman v. Bates*, 15 Vt. 51 (1843), but the issue was avoided by holding that the defendant was not liable because no force was used in the entry.

[183] 3 JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES 609 (1833).

Can we, that is, simply jettison the common-law precedents that provided the crucial framework for the Fourth Amendment's text? The dilemma is troubling, and gives good cause to look for middle ground. Before taking up that quest, let us consider the second aspect of common-law dynamism.

B. Statutory Revisions of Common-Law Rules

In England, if Parliament abrogated the common-law rule about liability attaching if stolen goods were not found, the statute would trump the common-law rule.[184] What, then, in the United States following ratification of the Fourth Amendment? If we think that *Beaty* was right to abrogate an unwise common-law doctrine, it would seem to follow that a legislature could abrogate the same rule by statute.

The early Congress enacted a variety of innovative limitations on the tort liability of federal revenue agents.[185] Notably, the 1791 Excise Act, in some ways more favorable to plaintiffs than the 1789 Revenue Act, cut off liability for warrantless searches on dry land given probable cause, even if the suspected articles were not discovered.[186] Indeed, the early Congress adopted a variety of statutory provisions limiting the liability of federal revenue officers. Professor Arcila identifies founding-era statutes:

> (1) [A]uthorizing officers to plead the general issue; (2) authorizing them to plead the President's rules in defense, or to submit into evidence the statutory act and its authorization for civil searches, as well as 'any special

---

[184] *See, e.g.*, BLACKSTONE, *supra* note 176, at *89 ("Where the common law and a statute differ, the common law gives place to the statute.").

[185] *See* Jerry L. Mashaw, *Recovering American Administrative Law: Federalist Foundations, 1787-1801*, 115 YALE L.J. 1256, 1330 (2006) ("[T]he Collection Act of 1789 tried to discourage baseless suits against federal officials by allowing them to recover double their costs if the plaintiff lost his suit. Moreover, the court was allowed to absolve the defendant by finding reasonable cause for a seizure, even if a jury verdict had declared it illegal. Congress placed a similar provision in the 1799 Act regulating collection of tonnage duty." (footnote omitted)).

[186] *See* Fabio Arcila, Jr., *The Framers' Search Power: The Misunderstood History of Suspicion & Probable Cause*, 50 B.C. L. REV. 363, 407 (2009) (1791 Excise Act created new probable-cause defense for warrantless searches on land).

> matter'; (3) granting successful defendants double or even treble costs; (4) authorizing the court to summarily adjudge the case; and (5) allowing removal of a case from state court even after judgment, with the federal court then proceeding de novo.[187]

The early Congress was especially fond of discouraging suits against customs officers by imposing double (in one instance triple) costs on losing plaintiffs.[188]

Where the searches subject to these rules were made on ships, the pre-constitutional law was admiralty rather than common law.[189] Whether the pre-constitutional law was common law or admiralty, the plethora of founding-era statutes limiting officer liability show that there was no original understanding of the Fourth Amendment as freezing the pre-constitutional tort law in 1791 form.

Just as with evolution by a course of judicial decisions, however, the flexibility provided by statutory changes comes at the price of determinacy. A statute immunizing complaining citizens, or police, when search under a valid warrant fails to turn up the stolen goods, does not seem unreasonable. What, however, about a statute that grants government agents *absolute immunity* for search and seizure? *Entick* held that the defendants were not entitled to the immunity conferred by statute on justices of the peace.[190] The statute apparently conferred only limited, rather than absolute, immunity.[191] Parliament, however, had power to both extend the immunity to executive officers and to provide absolute rather than limited protection.

The effect of the hypothetical statute is to give the FBI the same power as would be conferred by a general warrant. That has to be unconstitutional. So we return to our dilemma. If we treat the pre-constitutional law of search and seizure as ossified by the

---

[187] Arcila, *supra* note 180, at 1315 (footnotes omitted).

[188] *Id.*

[189] There was at least some application of these liability limits to common-law trespass actions. *See Id.* at 1305-06 (discussing application of 1791 Excise Act to searches of distilleries).

[190] Entick v. Carrington, 95 Eng. Rep. 807, 817-18 (C.P. 1765).

[191] *See* Pfander & Hunt, *supra* note 100, at 1928 n.290.

Fourth Amendment, we inflict bad policy on ourselves while defying the founding-era understanding that the common law was dynamic. If we say that the founding-era common law that gave the Fourth Amendment its context can be changed at will, we render the constitutional provision nugatory.

IV. DESCRIPTIVE BALANCE OF ADVANTAGE ACCOUNTS: ANALYSIS AND CRITIQUE

A. The Balance of Advantage Concept

Given the difficulty, even, perhaps, the impossibility, of deriving the original understanding of the Fourth Amendment from specific founding-era rules and practices, there is good reason to seek some other approach. The most plausible alternative is to look, not to specific founding-era rules, but to the scope of individual liberty and privacy that prevailed under the legal regime as a whole in the founding era. Justice Scalia took this approach in *Kyllo v. United States*.[192]

The issue in *Kyllo* was whether the use of a thermal-imager to read infrared radiation emitted from inside a home constituted a "search." At common law, Kyllo could not have sued the officer for trespass since there was no entry of his premises. Justice Scalia for the majority, however, balked at such a focus on the specific common-law tort rules, stating instead:

> We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search.[193]

---

[192] 533 U.S. 27 (2001).

[193] *Id.* at 34-35 (citation omitted).

Now this is at least a praise-worthy recognition of how the specific common-law rules reflected political values, values the rules may cease to serve when other facets of the legal ecology change. It sacrifices a measure of determinacy for a measure of flexibility. It yields, however, only an incomplete account of the original understanding, because it imputes to the founders the confusion of *is* and *ought*.

B. Descriptive Balance-of-Advantage Accounts: A Critique

The founders might have hoped for a different "degree of privacy against government" than the one "that existed when the Fourth amendment was adopted."[194] Indeed, the founding-era criminal justice system was not regarded as perfect by the founders. They changed some features of it with specific clauses like the Sixth Amendment Right to Counsel and Compulsory Process Clause. They instantiated some specific current practices with clauses such as the Confrontation Clause.

The Framers, however, held no uncritical reverence for the common law of crimes. For example, the first federal criminal code, adopted in 1790, eliminated capital punishment for larceny,[195] relaxed the pleading rules for indictments charging perjury,[196] and abolished the benefit of clergy.[197] We have already seen that the early revenue acts made extensive changes in the procedures for litigating tort suits against customs officers.[198]

The Fourth Amendment, however, does not instantiate the then-existing tort rules of trespass and false imprisonment. Nor does it replace them with any concrete reform. To read the general language as instantiating the 1791 levels of liberty and privacy is arbitrary. The founders might well have favored a different balance if the institutional, technological, and doctrinal resources to achieve a different balance had been available to them.

---

[194] *Id.* at 28.

[195] An Act for the Punishment of Certain Crimes Against the United States, ch. 9, Stat. 112, 116 § 16 (1790) (larceny punished by fine four times the value of stolen goods plus public whipping "not exceeding thirty-nine stripes").

[196] *Id.* § 19.

[197] *Id.* at 113 § 31.

[198] *See supra* notes 185-88 and accompanying text.

Think about what "the degree of privacy against government that existed when the Fourth Amendment was adopted" would actually mean. When the Fourth Amendment was adopted there were no pro-active professional police forces employing undercover agents or even engaged in pro-active patrol. Indeed, the absence of police and the private prosecution system left society's lower classes substantially unprotected by the criminal law.[199] And the adjudication system had evolved with the aim of nullifying capital punishment rather than rational fact-finding.

What's the point? The point is that the founders were not satisfied with their criminal justice system. They wanted one that would do more to protect public security without compromising individual freedom. Not until the nineteenth century would the wealth and the institutional sophistication emerge that would permit major increases in public security, increases that inevitably created some risk to individual liberty and privacy. The descriptive founding-era balance of advantage does not tell us that the founders would not have welcomed, as their posterity welcomed, the new instruments of social control such as the police and the penitentiary.

IV. ASPIRATIONAL BALANCE OF ADVANTAGE ORIGINALISM

Thus far I have argued that consulting specific common-law tort rules as a guide to the Fourth Amendment's meaning is a mistake, and that descriptive balance-of-advantage accounts are also mistaken. The strongest version of Fourth Amendment originalism is an *aspirational* balance of advantage originalism. This approach asks whether searches and seizures threaten the priority of individual liberty and privacy, as against public security, that the founders aspired to.

Now I frankly concede that this is not a very determinate criterion. But it is not a hopeless enterprise. First, we start from where we are today. When a case comes up that raises a new issue, or that calls upon the Supreme Court to reconsider precedent, we ask whether a ruling for one side or the other would move us closer to the privacy/security balance favored by the founders. Second, we can look to the specific rules and practices of the founding era as data points—as evidence of the aspirational balance of advantage.

---

[199] *See, e.g.*, JEREMY BENTHAM, ORGANIZATION OF JUDICIAL ESTABLISHMENTS IN IV WORKS 305, 391 (J. Bowring ed., 1843) ("Delinquency, which, whenever the law sleeps, is but the more vigilant and alert, takes note of all the conjectures when the situation of things refuses a voluntary prosecutor . . . where the parties concerned in interest are minors, females, absent, helpless, or insane, and the strongest suggests of interest are rendered fruitless by inability.").

I would, however, recognize both the profoundly different context of those specific practices and their dynamic nature. We need to recognize that rules for an amateur system may make no sense of a professional system of full-time, repeat players. We need to recall not just the rules, but the institutions, of founding-era criminal justice.

As to the dynamism point: With such founding-era practices as the ban on seizing documentary evidence and the stolen-goods-must-be-found-where-sought rule, I would treat the founding-era common-law cases with the same respect—no more, no less—than the Court treats its own constitutional precedents.[200] The founders knew the common law could change and that statutes could modify the decisional law. The usual criteria for overruling—changed circumstances, conflicting lines of precedent, public reliance, and so on—have as much practical bearing on pre-ratification as on post-ratification precedents. And those criteria make overruling *Entick* on the private papers point as legitimate as overruling *Boyd* on the same issue.

Statutory impositions on liberty and privacy pose a different challenge. From what has been said, it follows that a statute that overturns a founding-era rule should be held constitutional when the conditions exist that would justify judicial overruling of the founding-era practice. Beyond that, when a statute or executive practice trenches on liberty or privacy in the name of public security, aspirational balance of advantage enquires whether the statute or practice is consistent with the free society the Framers envisioned.

---

[200] As a matter of actual judicial practice, Chief Justice Rehnquist gave this rough and ready generalization: "While '*stare decisis* is not an inexorable command,' particularly when we are interpreting the Constitution, 'even in constitutional cases, the doctrine carries such persuasive force that we have always required a departure from precedent to be supported by some 'special justification.''" Dickerson v. United States, 530 U.S. 428, 443 (2000) (citations omitted). My own view is that in criminal procedure cases, a field where the law is predominantly judge-made constitutional law, the justices should overrule cases that have lost majority support rather than seize upon arbitrary distinctions to reach desired results. *See* Donald A. Dripps, *Constitutional Theory for Criminal Procedure: Dickerson, Miranda, and the Continuing Quest for Broad-but-Shallow*, 43 WM. & MARY. L. REV. 1, 39-46 (2001). As with most disputes about *stare decisis* as a general matter, the difference with the Court's formula is one of degree rather than kind.

George Thomas developed this basic approach by proposing a thought-experiment in which the Framers are given knowledge of modern conditions, especially modern policing.[201] My aspirational balance account differs in some ways. Thomas focused on Madison individually, and tried to imagine the amendment Madison would have written given prescience.[202] Aspirational balance looks to the expectations of the ratifying generation as a guide to interpreting the decidedly plastic language the founders adopted.

I freely concede that this approach lacks the value-neutral determinacy of, say, the price term in a contract. From a methodological point of view, the aspirational balance approach is little different from the second Justice Harlan's approach.[203] Justice Harlan was the father of modern stop-and-frisk doctrine.[204] Professor Thomas regards stop-and-frisk on less than probable cause as contrary to founding-era values.[205] The wise and learned, working hard and in good faith, will often disagree.

---

[201] George C. Thomas III, *Time Travel, Hovercrafts, and the Fourth Amendment: James Madison Sees the Future and Rewrites the Fourth Amendment*, 80 NOTRE DAME L. REV. 1451 (2005).

[202] *Id.*

[203] *See* Donald A. Dripps, *Justice Harlan on Criminal Procedure: Two Cheers for the Legal Process School*, 3 OHIO ST. J. CRIM. L. 125, 132 (2005) ("Harlan's fundamental commitment to legality followed the legal process school rather than any species of formalism. The Court should carefully consider the institutional advantages and disadvantages of Congress, the states, and the Court itself. For the most part, important policy choices should be left to the states and to Congress, but when the Court acted within the proper sphere of its institutional competence, the justices had no choice but to consider values as well as facts in reaching their decisions. History counted, but you will not find Harlan asking the Framers for answers to questions that never occurred to them." (footnote omitted)).

[204] *See* Terry v. Ohio, 392 U.S. 1, 31, 32-33 (1968) (Harlan, J., concurring).

[205] *See* Thomas, *supra* note 201, at 1515 ("As Justice Scalia reads the history (and as I read the history) a search, even a frisk, of a suspicious person on the street requires probable cause."). Thomas would permit automatic search incident to arrest,

So to the objection that the enquiry I propose is too amorphous, the only riposte I have is that in the Fourth Amendment context this is where originalism takes you—by one route among many to the same normative issues that are bound to determine outcomes under this kind of text with this kind of history.[206] History, precedent, and process theory can help discipline our normative deliberation, but they cannot excuse us from it, whatever our favored theory of constitutional interpretation.

CONCLUSION

An originalist approach to the Fourth Amendment based on specific founding-era practices is illogical and unwise. A search or seizure in 1791 took place in an institutional context so different from ours that it simply is not the same search or seizure it was then. The founders, moreover, understood the common law to be dynamic. The language they chose was crafted against a background they expected to evolve. They themselves tinkered extensively with the pre-constitutional tort law of searches and seizures.

Descriptive balance-of-advantage approaches, exemplified by *Kyllo*, are a promising response to the dual challenges of contextual change and common-law dynamism. The obvious problem with any approach that rejects ossification of the 1791 common law is determinacy. Aspirational balance-of-advantage originalism at least asks the right question about Fourth Amendment cases: Is the search or seizure at issue consistent with the balance of public security and individual freedom the founders hoped our society would achieve? If the quest for the original understanding, properly described by that question, leads

---

so if the Framers assumed the power *to arrest* those behaving suspiciously for vagrancy, *Terry* might actually give modern pedestrians more protections than was originally expected. *See supra* note 201 and accompanying text.

[206] Without asserting it, I am inclined to suppose that the point applies to constitutional law generally and not solely to constitutional criminal procedure. *See* Thomas B. Colby, *The Sacrifice of the New Originalism*, 99 GEO. L.J. 713 (2011) (arguing that the "new originalism" loses determinacy as it accounts for objections to the "old originalism").

to reasonable disagreements about modern facts and modern values, so be it.

REASONABLENESS WITH TEETH: THE FUTURE OF FOURTH AMENDMENT REASONABLENESS ANALYSIS

Cynthia Lee[*]

INTRODUCTION 1133
I. FOURTH AMENDMENT REASONABLENESS: THE PAST 1137
II. FOURTH AMENDMENT REASONABLENESS: THE PRESENT 1139
III. PROBLEMS WITH THE COURT'S CURRENT FOCUS ON REASONABLENESS 1147
  A. The Traditional Critique of Reasonableness 1147
  B. The Critique of Reasonableness From the Left 1150
IV. THE FUTURE: A HYBRID APPROACH 1157
CONCLUSION 1182

INTRODUCTION

Reasonableness standards permeate the law. From the reasonable man standard used to measure negligent behavior in tort law[1] to the requirement in criminal law that a person claiming self-defense must have reasonably believed that the force used was necessary to prevent an imminent unlawful attack,[2] the law demands more from us than simply our honest, good faith efforts. Across disciplines, the law requires that we act reasonably.

---

[*] Charles Kennedy Poe Research Professor of Law, The George Washington University Law School. A special thanks to Tom Clancy for inviting me to write and present this paper at the National Judicial College's Annual Fourth Amendment Symposium in Oxford, Mississippi in March 2011. I appreciate thoughtful comments on this paper by Eric Miller, Fabio Arcila, Jonathan Witmer-Rich, Josephine Ross, and David Gray when I presented it at Law and Society in San Francisco, California in June 2011. I thank Erin Mick for excellent research assistance. Parts of this Article have been adopted from Cynthia Lee, *Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us About the Fourth Amendment*, 100 J. CRIM. L. & CRIMINOLOGY 1403 (2010).

[1] RESTATEMENT (SECOND) OF TORTS § 283 (1965).

[2] *See, e.g.*, CYNTHIA LEE, MURDER AND THE REASONABLE MAN: PASSION AND FEAR IN THE CRIMINAL COURTROOM 131 (2003); Cynthia Kwei Yung Lee, *Race and Self-*

Just as reasonableness standards permeate the law in general, reasonableness standards permeate the law regarding the Fourth Amendment. The Supreme Court's definition of a "search" within the meaning of the Fourth Amendment turns on whether the defendant's expectation of privacy was *reasonable*.[3] The Court's definition of a "seizure" of the person turns on whether a *reasonable* person in the defendant's shoes would have felt free to leave or terminate the encounter with the police officer.[4] Probable cause to search is defined as *reasonable* grounds to believe that evidence of a crime will be found in the place to be searched.[5] Officers can conduct a *Terry* stop upon *reasonable* suspicion of criminal activity and can do a *Terry* frisk of the person if they have *reasonable* suspicion that the suspect is armed and dangerous.[6] And, increasingly, the validity of a search turns on whether the reviewing court believes the search was reasonable.[7]

Because reasonableness plays such an important role in Fourth Amendment search jurisprudence, this Article assesses the past, the present, and the future of reasonableness analysis. Part I focuses on the past. For much of the twentieth century, the Court embraced what is called the warrant preference view of the

---

Defense: Toward a Normative Conception of Reasonableness, 81 MINN. L. REV. 367 (1996).

[3] Katz v. United States, 389 U.S. 347 (1967).

[4] *See* Florida v. Bostick, 501 U.S. 429 (1991); United States v. Mendenhall, 446 U.S. 544 (1980).

[5] Maryland v. Pringle, 540 U.S. 366, 371 (2003) ("The substance of all the definitions of probable cause is a reasonable ground for belief of guilt . . . ." (quoting Brinegar v. United States, 338 U.S. 160, 175 (1949))); *see also* Kit Kinports, *Diminishing Probable Cause and Minimalist Searches*, 6 OHIO ST. J. CRIM. L. 649 (2009) [hereinafter Kinports, *Diminishing Probable Cause*] (opining that by using phrases like "reasonable belief" and "reason to believe," the Court risks conflating for probable cause and reasonable suspicion standards).

[6] Terry v. Ohio, 392 U.S. 1 (1968). As Lewis Katz notes, the *Terry* Court never used the term "reasonable suspicion." Lewis R. Katz, Terry v. Ohio *at Thirty-Five: A Revisionist View*, 74 MISS. L.J. 423, 486 (2004). The reasonable suspicion standard was articulated in Justice Harlan's concurring opinion in *Sibron v. New York*, 392 U.S. 40, 71 (1968) (Harlan, J., concurring).

[7] United States v. Knights, 534 U.S. 112 (2001).

Fourth Amendment under which the validity of a search turned on whether the police sought prior judicial authorization in the form of a warrant based on probable cause issued by a magistrate judge. In case after case, the Court would announce that searches "conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well delineated exceptions."[8] Under the warrant preference model of reasonableness, a search was considered reasonable if the government obtained a search warrant prior to the search or an exception to the warrant requirement applied.

Part II focuses on the present. Even though it still treats as reasonable both searches conducted pursuant to a warrant and searches that fall within a well-established exception to the warrant requirement, the modern Court has increasingly abandoned the warrant preference view. Instead of interpreting the Fourth Amendment as expressing a preference for warrants, the modern Court reads the text of the Fourth Amendment as simply requiring reasonableness.[9] Under this textualist reading of the Fourth Amendment, commonly called the reasonableness view, a search or seizure is valid as long as it is reasonable.[10] The Court, however, has provided lower courts with little guidance as to what makes a search or seizure reasonable, suggesting only that whether a search is reasonable requires a balancing of the government's interests against the individual's interests.[11] Reasonableness as balancing gives lower courts overly broad discretion to decide whether a search or seizure is reasonable.

In a number of fairly recent cases, the modern Court has slightly revised the way it assesses the reasonableness of a search. In an effort to provide more guidance to lower courts, it has adopted what some have called an originalist approach.[12] Under this approach, a reviewing court must first ask whether the challenged governmental action was unlawful under the common law at the time of the Constitution's framing.[13] If so, then it will be considered unreasonable.[14] If it is unclear whether the challenged governmental action was unlawful at the time of the framing, the reviewing court goes back to a balancing test, balancing the government's interests against the individual's interests.[15]

---

[8] Minnesota v. Dickerson, 508 U.S. 366, 372 (1993); Coolidge v. New Hampshire, 403 U.S. 443, 454-55 (1971); *Katz*, 389 U.S. at 357.

[9] Florida v. Jimeno, 500 U.S. 248, 250 (1991) ("The Fourth Amendment does not proscribe all state-initiated searches and seizures; it merely proscribes those which are unreasonable.").

[10] *See infra* Part II.

[11] *Knights*, 534 U.S. at 118-19 ("The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined by [balancing].").

Part III critiques the Court's current focus on reasonableness as the touchstone of Fourth Amendment analysis. It starts with what might be called the traditional critique of reasonableness. Under this critique, the current reasonableness inquiry is problematic because it provides insufficient guidance to lower courts and results in rulings that tend to be overly deferential to the government. Part III also provides the left critique of reasonableness. Under this critique, open-ended reasonableness balancing is problematic because it enables subconscious biases to influence the decision-making process both on the ground and in the courtroom. Implicit bias may lead police officers to see young men of color on the street as more suspicious than others, which may lead them to stop and search those individuals more frequently than others. Implicit bias may also lead courts to exercise their discretion to decide whether a search is reasonable in ways that favor law enforcement and disfavor blacks and Latinos who make up the bulk of individuals arrested, tried, and convicted of crimes in the United States.

Part IV looks to the future. The Court today stands at a crossroads. It can completely replace the warrant preference model with the reasonableness model of the Fourth Amendment, as it has already done in a few cases, it can return to a robust embrace of the warrant preference view, or it can recognize the virtues of the warrant preference and the reasonableness models and improve upon both. I support continued adherence to the warrant preference view, but recognize that the Court is unlikely to return to a robust embrace of warrants. In light of this reality, I argue that the Court should continue its current path of recognizing both models. Instead of extremely deferential pro-government reasonableness balancing, however, courts should engage in a more stringent form of reasonableness review, review that I call "reasonableness with teeth."[16]

---

[12] David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739, 1760 (2000).

[13] Wyoming v. Houghton, 526 U.S. 295, 299 (1999).

[14] *Id.* at 299-300.

[15] *Id.*

I. FOURTH AMENDMENT REASONABLENESS: THE PAST

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[17]

Criminal procedure scholars and the Justices of the Supreme Court have debated the meaning of these words for years. The debate has centered on whether to interpret the Fourth Amendment as one interconnected text or as two separate clauses. As Justice Clarence Thomas explained in his dissent in *Groh v. Ramirez*, "The precise relationship between the Amendment's Warrant Clause and Unreasonableness Clause is unclear. . . . [T]he Court has vacillated between imposing a categorical warrant requirement and applying a general reasonableness standard."[18]

---

[16] I am not the first to suggest a more rigorous form of Fourth Amendment reasonableness review, see Clancy, *The Fourth Amendment's Concept of Reasonableness*, *infra* note 28, and Colb, *The Qualitative Dimensions of Fourth Amendment "Reasonableness," infra* note 66, and I am not the first to borrow from the concept of rational basis with bite in the equal protection arena. Christopher Slobogin has suggested that "Fourth Amendment analysis should mimic equal protection rationality review 'with bite,' if not strict scrutiny." CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 42 (2007) [hereinafter SLOBOGIN, PRIVACY AT RISK]. Slobogin proposes a two-tiered framework involving a proportionality principle and an exigency principle, which I discuss later in this paper. *See infra* text accompanying notes 171-82.

[17] U.S. CONST. amend. IV.

[18] Groh v. Ramirez, 540 U.S. 551, 571-72 (Thomas, J., dissenting).

For much of the twentieth century, the Supreme Court embraced the warrant preference view of the Fourth Amendment, under which the validity of a search turned on the presence or absence of a search warrant.[19] Under the warrant preference view of the Fourth Amendment, if the officer obtains advance judicial authorization for a search in the form of a search warrant or if a search falls within one of the exceptions to the warrant requirement, the search will be presumed reasonable. Adherents of the warrant preference view emphasize the importance of having a neutral, detached judicial officer, rather than a police officer, make the probable cause determination.[20]

In response to the argument that the text of the Fourth Amendment does not require warrants or probable cause, proponents of the warrant preference view read the two clauses in the Fourth Amendment as interconnected and related. As Morgan Cloud explains, the warrant preference view employs a conjunctive theory that links the two clauses in the Fourth Amendment together such that a search is considered reasonable if it was conducted pursuant to a warrant or an exception to the warrant requirement applied.[21]

Proponents of the warrant preference view also look to history to support their interpretation of the Fourth Amendment. They point out that the framers were primarily interested in protecting citizens against "arbitrary deprivations of privacy, property, and liberty."[22] Accordingly, when they drafted the

---

[19] Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 559 (1999) ("For most of [the twentieth] century, the Supreme Court has endorsed what is now called the 'warrant-preference' construction of Fourth Amendment reasonableness, in which the use of a valid warrant . . . is the salient factor in assessing the reasonableness of a search or seizure."); James J. Tomkovicz, California v. Acevedo: *The Walls Close in on the Warrant Requirement*, 29 AM. CRIM. L. REV. 1103, 1124 (1992) ("For most of the twentieth century, the Court has proclaimed its faith in the principle of neutral, judicial screening of executive decisions to search.").

[20] *Id.* at 1164 ("Neutral judicial determinations seem far preferable to those made by interested law enforcement agents."); *see also* United States v. Chadwick, 433 U.S. 1, 9 (1977).

[21] Morgan Cloud, *Searching through History; Searching for History*, 63 U. CHI. L. REV. 1707, 1721-22 (1996) (reviewing William John Cuddihy, The Fourth Amendment: Origins and Original Meaning 602-1791 (1990) (unpublished Ph.D. dissertation, Claremont Graduate School) (on file with UMI Dissertation Service)).

[22] Tomkovicz, *supra* note 19, at 1134.

Fourth Amendment, the framers sought to constrain executive discretion by subjecting search and seizure decisions to judicial control.[23] While the framers may have focused primarily on the evils of general warrants and writs of assistance, they would have been equally concerned with warrantless searches had such searches been more common at that time because such searches would have resulted in similar harms.[24]

Proponents of the warrant preference view argue that a warrant requirement with well-delineated exceptions provides more clarity than a general requirement that searches and seizures not be unreasonable.[25] Police officers can more easily predict whether their actions will be considered constitutional under the warrant preference view than under an interpretation of the Fourth Amendment that just tells them they need to act "reasonably."[26] This is because if they procure a warrant, there is little question that the subsequent search will be deemed valid.

II. FOURTH AMENDMENT REASONABLENESS: THE PRESENT

In contrast to the warrant preference view is what I call the separate clauses view, or what most call the reasonableness view, of the Fourth Amendment. Supporters of this view focus on the word "and" in the middle of the Fourth Amendment.[27] They argue that the text of the Fourth Amendment is clearly divided into two separate and completely independent clauses—one stating that searches and seizures must not be unreasonable; the other specifying the requirements for a valid warrant.[28] Supporters of the reasonableness view argue that the original intent of the Framers "was to outlaw certain kinds of warrants [general warrants], not to enact a preference for warrants."[29]

---

[23] *Id.*

[24] *Id.* at 1135.

[25] *Id.* at 1155.

[26] *Id.*

[27] Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 759 (1994); Fabio Arcila, Jr., *The Death of Suspicion*, 51 WM. & MARY L. REV. 1275, 1280-88 (2010) [hereinafter Arcila, *The Death of Suspicion*]; Fabio Arcila, Jr., *In the Trenches: Searches and the Misunderstood Common-Law History of Suspicion and Probable Cause*, 10 U. PA. J. CONST. L. 1, 8 (2007) [hereinafter Arclia, *In the Trenches*].

[28] Amar, *supra* note 27, at 762 (noting that "[t]he Amendment contains two discrete commands—first, all searches and seizures must be reasonable; second, warrants authorizing various searches and seizures must be limited (by probable cause, particular description, and so on)"); *see also* Ricardo J. Bascuas, *Fourth Amendment Lessons from the Highway and the Subway: A Principled Approach to*

Under the reasonableness view, a search comports with the Fourth Amendment as long as it is reasonable.[30] The validity or reasonableness of the search does not turn on whether the government obtained a search warrant prior to the search.[31] Searches and seizures conducted without a warrant are valid as long as they are reasonable.[32] The probable cause requirement applies only when police seek a warrant.[33] Reasonableness review consists of balancing the governmental interests against the individual's interests.[34]

Suspicionless Searches, 38 RUTGERS L.J. 719, 724-25 (2007) (explaining that supporters of the reasonableness view of the Fourth Amendment "argue that the plain text reveals no grammatical or logical relationship between the Warrant Clause and the Reasonableness Clause"); Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977, 999 [hereinafter Clancy, *The Fourth Amendment's Concept of Reasonableness*] (explaining that under the reasonableness view, "the Fourth Amendment's two clauses are distinct: the first clause requires only that searches and seizures be 'reasonable'; the second clause addresses only those searches and seizures conducted under warrants . . ."); Tracey Maclin & Julia Mirabella, *Framing the Fourth*, 109 MICH. L. REV. 1049, 1061 (2011) (reviewing William John Cuddihy, The Fourth Amendment: Origins and Original Meaning 602-1791 (1990) (unpublished Ph.D. dissertation, Claremont Graduate School) (on file with UMI Dissertation Service)) (explaining that under the reasonableness view, the first clause "declares a freedom from unreasonable searches and seizures" while the second clause "specifies the form and content of search and arrest warrants").

[29] Tomkovicz, *supra* note 19, at 1130-31.

[30] Amar, *supra* note 27, at 759.

[31] *Id.*; *see also* Richard A. Posner, *Rethinking the Fourth Amendment*, 1981 SUP. CT. REV. 49, 72 ("The natural reading of the [Fourth] amendment is that unreasonable searches and seizures are forbidden (clause 1), and specifically (clause 2) that a search (or arrest) warrant is invalid unless it complies with the specific requirements (probable cause, etc.) spelled out in the second clause.").

[32] TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 43 (1969).

[33] Amar, *supra* note 27, at 782 ("The 'probable cause' standard applies only to 'warrants,' not all 'searches' and 'seizures.'"); Arcila, *The Death of Suspicion*, *supra* note 27, at 1294 ("*Only the Warrant Clause contains any textual support for a suspicion requirement* . . . .").

[34] Daniel S. Lohse, *Returning to Reasonableness: The Argument Against Expanding Investigatory Searches and Seizures to Completed Misdemeanors*, 2010 U. ILL. L. Rev. 1629, 1646; Alexander A. Reinert, *Public Interest(s) and Fourth Amendment Enforcement*, 2010 U. ILL. L. Rev. 1461, 1467 & 1469; Scott E. Sundby, *"Everyman" 's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1796-97 (1994).

The legislative history does not provide robust support for the separate clauses view of the Fourth Amendment. As Tom Clancy observes, the initial draft of the Fourth Amendment, prepared by James Madison, provided:

> The rights of the people to be secured in their persons, their houses, their papers, and their other property, from all unreasonable searches and seizures, *shall not be violated by warrants* issued without probable cause, supported by oath or affirmation, or not particularly describing the places to be searched, or the persons or things to be seized.[35]

In other words, it appears that the Framers were primarily concerned with preventing warrants issued without probable cause. They viewed as unreasonable searches and seizures conducted pursuant to such warrants. The initial draft of the Fourth Amendment clearly linked the two clauses together such that the prohibition against unreasonable searches and seizures was violated when a warrant was issued without probable cause and without particularity of description.

According to Clancy, the initial draft of the Fourth Amendment was referred to the Committee of Eleven, which consisted of one congressman from each state represented in Congress.[36] The Committee revised the draft as follows: "The rights of the people to be secured in their persons, houses, papers, and effects, *shall not be violated by warrants* issuing without probable cause, supported by oath or affirmation, and not particularly describing the place to be searched, and the persons or things to be seized."[37]

The amended draft, like the original draft, linked the two clauses such that the rights protected by the Fourth Amendment would be violated if a warrant was issued without probable cause or particularity of description. Clancy notes that one Egert Benson of New York objected to the phrase "by warrants issuing" and wanted to replace these words with "and no warrant shall issue" because he felt the draft language was not forceful enough to convey the Framer's strong disapproval of general warrants.[38] Benson's proposal was defeated by a "considerable majority" of the House, but Benson, as chair of the committee that reported amendments out to the Senate, inserted this clause into the final draft.[39] Somehow this change went unnoticed and the Fourth Amendment, as amended by Benson, was formally enacted.[40] Benson's original intent may have been to bolster the idea that searches pursuant to general warrants, i.e., warrants issued without probable cause or not particularly describing the place to be searched or the person or things to be seized, were unreasonable, but proponents of the reasonableness view have interpreted the phrase "and no warrants shall issue" as divorcing the prohibition against unreasonable searches and seizures from the requirements of a valid warrant.

---

[35] Thomas K. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483, 515 (1995) (citing 1 ANNALS OF CONG. 452 (1789)) (emphasis added).

[36] *Id.* at 516.

[37] *Id.* (emphasis added). The Committee of Eleven's draft did not include any reference to "unreasonable searches and seizures." *Id.* Clancy notes that this omission was inadvertent and the phrase was later re-inserted into the draft that became the Fourth Amendment as we know it today. *Id.*

The reasonableness view of the Fourth Amendment was promoted by Akhil Amar in his 1994 *Harvard Law Review* article, *Fourth Amendment First Principles*.[41] In this article, Amar argued the text of the Fourth Amendment does not require warrants or even probable cause.[42] According to Amar, all the Fourth Amendment requires is that searches and seizures be reasonable, or at least not unreasonable.[43] While the reasonableness approach was reflected in a few pre-1994 Supreme Court opinions,[44] Amar's work hastened its prominence. Over the past several decades, the Court has increasingly embraced the reasonableness view of the Fourth Amendment. In case after case, the Court has announced that "the touchstone of the Fourth Amendment is reasonableness."[45] Since 2000, only a few decisions have explicitly embraced the warrant preference view, the most recent of which was *Arizona v. Gant*, authored by former Supreme Court Justice John Paul Stevens.[46] With Justice Stevens's departure from the Court in 2010, the number of decisions strongly embracing the warrant preference view is likely to diminish even further.

---

[38] *Id.*

[39] *Id.*

[40] *Id.* at 516-17.

[41] Amar, *supra* note 27.

[42] *Id.* at 761.

[43] *Id.* at 801.

[44] Thomas Y. Davies, *The Supreme Court Giveth and the Supreme Court Taketh Away: The Century of Fourth Amendment "Search and Seizure" Doctrine*, 100 J. CRIM. L. & CRIMINOLOGY 933, 937 (2010) (noting that "in the 1925 ruling in *Carroll v. United States*, [the Supreme Court] adopted the view that the Fourth Amendment did not condemn all warrantless searches, but only those that the justices did not find to be 'reasonable' in the circumstances"). Some scholars point to two cases in the 1960s—*Camara v. Municipal Court* and *Terry v. Ohio*—as marking the beginning of the Court's turn away from the warrant preference view and its embrace of reasonableness

Another model of reasonableness that has started to emerge primarily in the opinions of Justice Scalia and Justice Thomas is what David Sklansky calls the Court's "new Fourth Amendment originalism."[47] This approach, which can be considered a subset of the reasonableness view, appears to limit the discretion of reviewing courts by requiring them to look to common law precedent. As Justice Scalia explains, the Court must construe Fourth Amendment reasonableness in terms of what was considered an unreasonable search when the Fourth Amendment

---

balancing. *See, e.g.*, Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of* Camara *and* Terry, 72 MINN. L. REV. 383, 385 (1988) ("[T]his Article traces the Court's fourth amendment analysis from the warrant clause's dominance through the eventual enthronement by *Camara* and *Terry* of the reasonableness balancing test."); Reinert, *supra* note 34, at 1468-69 (opining that *Camara* and *Terry* "signaled the beginning of the end of the Warrant Clause's centrality to Fourth Amendment inquiries").

[45] *See, e.g.*, Brigham City v. Stuart, 547 U.S. 398, 403 (2006) ("[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness' . . . ."); United States v. Knights, 534 U.S. 112, 118–19 (2001) ("The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined by [balancing]."); Illinois v. McArthur, 531 U.S. 326, 330 (2001) ("[The Fourth Amendment's] 'central requirement' is one of reasonableness."); Soldal v. Cook County, 506 U.S. 56, 71 (1992) ("[R]easonableness is still the ultimate standard under the Fourth Amendment."); Florida v. Jimeno, 500 U.S. 248, 250 (1991) ("The Fourth Amendment does not proscribe all state-initiated searches and seizures; it merely proscribes those which are unreasonable.").

[46] Arizona v. Gant, 129 S. Ct. 1710, 1716 (2009) ("Consistent with our precedent, our analysis begins, as it should in every case addressing the reasonableness of a warrantless search, with the basic rule that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.'" (quoting Katz v. United States, 389 U.S. 347, 357 (1967))).

[47] *See* Sklansky, *supra* note 12, at 1760.

was adopted in 1791.[48] Under this focus-on-the-common-law-history approach, the reviewing court is supposed to first ask whether the challenged conduct was regarded as an unlawful search or seizure under the common law at the time when the Fourth Amendment was adopted.[49] If the governmental activity in question would have been unlawful at the time of the framing, it will be deemed unreasonable and in violation of the Fourth Amendment.[50] If it is unclear whether the challenged conduct was regarded as an unlawful search or seizure under the common law, then the reviewing court must go back to assessing the reasonableness of the search by balancing the intrusion on privacy against the promotion of legitimate governmental interests.[51]

Many believe the focus-on-the-common-law-history approach allows the Justices to reach the results they favor without appearing to be engaging in ideological favoritism.[52] In Thomas Davies's view, the common-law approach provides easy cover for the Justices to say that searches they want to approve are reasonable and searches they want to disapprove are unreasonable while appearing to reach these conclusions in a fair and neutral way.[53] Davies doubts "whether even clear history can provide much positive guidance for shaping specific responses to modern search and seizure issues."[54] This is because "[a]pplying the original meaning of the language of the Fourth Amendment in a completely changed social and institutional context would subvert the *purpose* the Framers had in mind when they adopted the text."[55] Likewise, Donald Dripps notes that "too much has changed to enable modern judges to seek specific guidance from eighteenth-century common law practices."[56] Morgan Cloud has observed that the common-law approach is partial in two ways: (1) it is incomplete, "reviewing only a small fraction of the relevant historical data;"[57] and (2) it is "partisan, selectively deploying fragments of the historical record to support their arguments about the Amendment's meaning."[58] David Sklansky suggests two additional problems with the common-law approach to reasonableness. First, because early common-law authority is widely indeterminate, the approach allows the Court to pick and choose which precedent it wishes to follow.[59] Second, since the framers were not necessarily concerned with issues regarding

---

[48] Wyoming v. Houghton, 526 U.S. 295, 299-300 (1999) ("In determining whether a particular governmental action violates [the Fourth Amendment], we inquire first whether the action was regarded as an unlawful search or seizure under the common law when the Amendment was framed."); *see also* United States v. Jones, 132 S. Ct. 945, 950 (2012) ("At bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'").

[49] Minnesota v. Dickerson, 508 U.S. 366, 379-80 (1993) (Scalia, J., concurring).

[50] *Id.*

[51] *Houghton*, 526 U.S. at 299-300.

[52] *See, e.g.*, Thomas Y. Davies, *Can You Handle the Truth? The Framers Preserved Common-Law Criminal Arrest and Search Rules in "Due Process of Law"—"Fourth Amendment Reasonableness" Is Only a Modern, Destructive, Judicial Myth*, 43 TEX. TECH L. REV. 51, 55-56 (2010) [hereinafter Davies, *Can You Handle the Truth?*] (opining that when the Justices of the Supreme Court have looked to framing era common-law doctrine to assess the reasonableness of a search or an arrest, "they have frequently misstated the historical doctrine in ways that fit the desired result"); *see also* Ronald J. Bacigal, *Making the Right Gamble: The Odds on Probable Cause*, 74 MISS. L.J. 279, 287 (2004) (noting that "Judge Richard Posner has been particularly critical of this 'originalist' approach, suggesting that it is a sham, with a 'judge . . . do[ing] the wildest things, all the while presenting himself as the passive agent of the sainted Founders—don't argue with me, argue with Them'").

[53] Davies, *Can You Handle the Truth?*, *supra* note 52, at 53 ("Notwithstanding recent originalist rhetoric, the actual course of search-and-seizure decisions reveals

---

that the justices of the Supreme Court have made arrest and search decisions on the basis of the majority's ideological predilections and then have sometimes advanced or concocted historical claims to justify their decisions.").

[54] Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 736 (1999).

[55] *Id.* at 740-41.

[56] Donald A. Dripps, *The Fourth Amendment and the Fallacy of Composition: Determinacy Versus Legitimacy in a Regime of Bright-Line Rules*, 74 MISS. L.J. 341, 409 (2004).

[57] Cloud, *supra* note 21, at 1707-08.

[58] *Id.* at 1708.

[59] Sklansky, *supra* note 12, at 1794. The Court itself acknowledged this problem in the *Atwater* case. *See* Atwater v. City of Lago Vista, 532 U.S. 318 (2001). In that case, a police officer arrested a woman named Gail Atwater for driving without a seatbelt, a fine only offense. Atwater was taken into custody and held in a jail cell until she was brought before a magistrate and released on bond. Ultimately, she was ordered to pay a $50 fine. Atwater brought a civil rights suit, alleging that the warrantless arrest for a fine only seatbelt violation constituted an unreasonable seizure under the Fourth Amendment. Atwater argued that police at early common law lacked the authority to make a warrantless arrest for a minor offense other than an offense involving breach of the peace. The Court rejected Atwater's argument and upheld the warrantless arrest. Justice Souter, writing for the Court, examined early common law and framing era authorities on police power to execute warrantless arrests and concluded that "the common law commentators (as well as the sparsely reported cases) reached divergent conclusions" on this issue. *Id.* at 328.

race, class, and gender, a focus on what was considered lawful at early common law might lead a reviewing court to overlook equality concerns.[60]

Ironically, even though today's Court does not accord the warrant preference view the premier status it once held, the Court still applies it in the bulk of its cases. If a search takes place with a valid search warrant, its constitutionality is presumed. If the government engages in a warrantless search and that search satisfies the requirements of a well-delineated exception to the warrant requirement, it too will be presumed reasonable. For example, in its recent 2011 decision in *Kentucky v. King*,[61] the Court paid credence to both views of the Fourth Amendment. Writing for the Court, Justice Alito started by expressing adherence to the reasonableness view of the Fourth Amendment, noting, "The text of the Amendment thus expressly imposes two requirements. First, all searches and seizures must be reasonable. Second, a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity."[62] In the very next paragraph, Justice Alito paid credence to the warrant preference view, noting, "It is a basic principle of Fourth Amendment law, . . . that searches and seizures inside a home without a warrant are presumptively unreasonable."[63] Justice Alito even acknowledged that the warrant requirement is subject to certain exceptions, including the exigent circumstances exception that was at issue in the case.[64]

The Court today stands at a crossroads. It can return to a robust embrace of warrants, it can completely abandon the presumption of reasonableness that currently accompanies searches that take place with a search warrant and searches that fall within an exception to the warrant requirement, and instead require reasonableness balancing in all cases in which a search is challenged, or it can continue to recognize the merits of both the warrant preference and reasonableness views. Given its current composition, the Court is unlikely to return to a robust embrace of the warrant preference view. Abandoning years of carefully developed Fourth Amendment doctrines, however, would be a mistake. The Court should recognize the strength of both models and improve upon their weaknesses. In the next Section, I outline why the Court should not completely replace the warrant preference model with the reasonableness model. In Part IV, I suggest that Fourth Amendment reasonableness review should be more rigorous and less deferential to the government than it is at present. In short, I propose that courts engage in reasonableness review *with teeth.*

---

[60] Sklansky, *supra* note 12, at 1772-73.

[61] 131 S. Ct. 1849, 1856 (2011).

[62] *Id.*

[63] *Id.* (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)) (internal quotation marks omitted).

[64] *Id.*

III. PROBLEMS WITH THE COURT'S CURRENT FOCUS ON REASONABLENESS

A. The Traditional Critique of Reasonableness

The modern Court's movement away from warrants and its embrace of reasonableness as the central meaning of the Fourth Amendment is problematic for several reasons. First, reasonableness review as currently applied in the Fourth Amendment context is highly deferential, resulting in decisions that usually uphold the challenged governmental action.[65] As Tom Clancy has noted, when the Court engages in reasonableness balancing, instead of being evenhanded, it balances with its thumb on the scale in favor of the government.[66] Fourth

---

[65] *See, e.g.*, Illinois v. Lidster, 540 U.S. 419 (2004); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995); Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990); Nat'l Treasury Emp. Union v. Von Raab, 489 U.S. 656 (1989); Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602 (1989); United States v. Montoya De Hernandez, 473 U.S. 531 (1985); New Jersey v. T.L.O., 469 U.S. 325 (1985); United States v. Martinez-Fuerte, 428 U.S. 543 (1976); Camara v. Municipal Court, 387 U.S. 523 (1967).

[66] Clancy, *The Fourth Amendment's Concept of Reasonableness*, *supra* note 28, at 1011; *see also* Sherry F. Colb, *The Qualitative Dimension of Fourth Amendment "Reasonableness,"* 98 COLUM. L. REV. 1642, 1687 (1998) [hereinafter Colb, *The Qualitative Dimensions of Fourth Amendment "Reasonableness"*] (noting that in cases where the Court engages in reasonableness balancing, it applies a "relaxed and deferential approach"); *Montoya De Hernandez*, 473 U.S. at 558 (Brennan, J., dissenting) (criticizing Fourth Amendment reasonableness balancing as a process "in

Amendment reasonableness review is so deferential to the government that some scholars have compared Fourth Amendment reasonableness review to rational basis review in the equal protection context.[67] Tracey Maclin, for example, notes that if the reviewing court "can identify any plausible goal or reason that promotes law enforcement interests," the challenged police conduct will often be considered reasonable and not in violation of the Fourth Amendment.[68]

While it may make sense to defer to the government when the court is reviewing social and economic legislation that does not impact a suspect class or fundamental right, which is what courts usually do when applying rational basis review, reasonableness review in the Fourth Amendment context should not be deferential to the government. Fear of arbitrary searches and a desire to check the discretion of searching governmental officials prompted the Framers to include the Fourth Amendment in the Bill of Rights in the first place.[69] The judiciary should be careful to defend its role of checking the executive when a fundamental right is at issue, especially when the bulk of individuals negatively impacted are poor persons of color.[70]

---

which the judicial thumb apparently will be planted firmly on the law enforcement side of the scales").

[67] Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 199 (1993) [hereinafter Maclin, *The Central Meaning of the Fourth Amendment*] ("Fourth Amendment questions are resolved using a test that approximates the rational basis standard, which is the test used to decide equal protection and due process challenges to social and economic legislation."); William J. Stuntz, *Implicit Bargains, Government Power, and the Fourth Amendment*, 44 STAN. L. REV. 553, 554 (1992) ("The Supreme Court's generalized 'reasonableness' standard resembles . . . rational-basis constitutional review . . . .").

[68] Maclin, *The Central Meaning of the Fourth Amendment*, *supra* note 67, at 200.

[69] *Id.* at 201 (opining that "the central meaning of the Fourth Amendment is distrust of police power and discretion").

[70] I. Bennett Capers, *Policing, Race, and Place*, 44 HARV. C.R.-C.L. L. REV. 43, 65 (2009) ("The collateral consequences of *Terry* and its progeny is that they permit the disproportionate targeting of minorities in cars, on buses, on planes, on foot, even in shopping malls."); Devon W. Carbado, *(E)Racing the Fourth Amendment*, 100 MICH. L. REV. 946, 977, 1030 (2002) (explaining why police are more likely to stop black people than white people when there is a choice between stopping one or the other); M. Chris Fabricant, *War Crimes and Misdemeanors: Understanding "Zero-Tolerance" Policing as a Form of Collective Punishment and Human Rights Violation*, 3 DREXEL L. REV. 373, 387-88 (2011) (noting that in New York City, police focus their attention on "poor communities of color" and that "[o]f the approximately 580,000 people stopped and

A second problem with the Court's embrace of reasonableness is that the Court has failed to define reasonableness for Fourth Amendment review purposes, except to say that a search may be considered unreasonable if it was unlawful at the time of the framing.[71] As a general matter, reasonableness review means the reviewing court must balance the government's interests against the individual's interests with little guidance from above.[72] Because the reviewing court is free to consider any circumstance it feels is relevant and disregard any circumstance it feels is irrelevant, the exercise of its unguided discretion can lead to inconsistent results. Many legal scholars have complained that since there are no standards to guide the court's discretion, searches and seizures are reasonable under the reasonableness view if the reviewing court thinks they are reasonable.[73]

The lack of guidance in Fourth Amendment reasonableness review is particularly striking given that on numerous occasions the Court has spoken of the importance of having bright line rules

---

searched in New York City in 2009, nearly 90% were black or Latino, yet they were less likely to have committed an offense than white people"); Jeffery Fagan & Garth Davies, *Street Stops and Broken Windows: Terry, Race, and Disorder in New York City*, 28 FORDHAM URB. L.J. 457, 458, 477 (2000) (noting "individuals of color are more likely than white Americans to be stopped, questioned, searched, and arrested" and referencing a New York City OAG Report showing "that stops were disproportionately concentrated in the city's poorest neighborhoods, neighborhoods with high concentrations of racial minorities"); David A. Harris, *Factors for Reasonable Suspicion: When Black and Poor Means Stopped and Frisked*, 69 IND. L.J. 659, 681 (1994) (noting that poor law-abiding African Americans and Hispanics living in high crime areas are subject to search and seizure much more often than are whites); Kevin R. Johnson, *How Racial Profiling in America Became the Law of the Land:* United States v. Brignoni-Ponce *and* Whren v. United States *and the Need for Truly Rebellious Lawyering*, 98 GEO. L.J. 1005, 1047 (2010) ("Police regularly stop and search Blacks and Latina/os in larger numbers than their percentage of the general population . . . [and] these minority groups represented the overwhelming majority of searches (77.2%).").

[71] *See supra* text accompanying notes 47-51.

[72] *See supra* text accompanying notes 34, 51.

[73] Davies, *Can You Handle the Truth?*, *supra* note 52, at 55 ("The beauty of 'Fourth Amendment reasonableness'—at least from the justices' points of view—is that it can carry whatever content the justices choose to give it."); Gerald S. Reamey, *When "Special Needs" Meet Probable Cause: Denying the Devil Benefit of Law*, 19 HASTINGS CONST. L.Q. 295, 299-300, 327 (1992) (arguing the reasonableness standard results in ad-hoc and unprincipled decision making); Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 855 (1994) (arguing that the "freewheeling 'reasonableness' standard . . . suffers from the concerns about official arbitrariness").

in the Fourth Amendment context to guide police officers who often need to make quick, on the spot decisions in the field.[74] When it comes to providing guidance to lower courts struggling to determine the validity of a search, however, the Court has eschewed bright-line rules in favor of a vague and amorphous reasonableness standard.

B. The Critique of Reasonableness From the Left

Beyond the traditional critique of reasonableness, both feminist theory and critical race theory offer additional insights. First, in purporting to be neutral and objective, a reasonableness standard can mask the fact that what the law considers reasonable is often just what those in positions of authority consider to be reasonable. As Dana Raigrodski notes, "reasonableness and common sense have always been assigned a race (white), a gender (male), and a class (wealthy)."[75]

Gender, religion, race, class, and sexual orientation, to name just a few markers of identity, can influence not only the way one experiences life, but also the way one perceives the world. Judges ascribing to a colorblind model of jurisprudence might not fully appreciate the ways in which race and ethnicity may influence assessments of suspicion and criminality. An example of this can be seen in Anthony Thompson's critique of the *Terry v. Ohio* decision.[76] In *Terry*, the Court held that an officer's decision to stop and frisk three men was not in violation of the Fourth Amendment, even though the officer lacked probable cause to believe they were involved in criminal activity.[77] The *Terry* Court established a new lower level of justification, later called reasonable suspicion, for brief investigatory seizures of the person.[78] Chief Justice Warren, writing the majority opinion in *Terry*, recounted the facts of the case in entirely race-neutral terms, never revealing that Terry and one of his companions were black, and that Terry's other companion and Detective McFadden were white.[79] Thompson suggests that only when one considers race does Detective McFadden's assertion—that he couldn't say what precisely drew his attention to the defendants and that he just didn't like them—make sense.[80]

---

[74] New York v. Belton, 453 U.S. 454 (1981); United States v. Robinson, 414 U.S. 218 (1973). For critiques of the Court's embrace of bright line rules, see Dripps, *The Fourth Amendment and the Fallacy of Composition*, *supra* note 56; Albert W. Alschuler, *Bright-Line Fever and the Fourth Amendment*, 45 U. PITT. L. REV. 227 (1984).

[75] Dana Raigrodski, *Reasonableness and Objectivity: A Feminist Discourse of the Fourth Amendment*, 17 TEX. J. WOMEN & L. 153, 187 (2008).

[76] Anthony C. Thompson, *Stopping the Usual Suspects: Race and the Fourth Amendment*, 74 N.Y.U. L. REV. 956 (1999).

[77] Terry v. Ohio, 392 U.S. 1 (1968).

Terry v. Ohio is not the only opinion in which the Court describes the facts of the case in entirely race-neutral terms. In countless Supreme Court cases, the race of the defendant is never mentioned, as if irrelevant.[81] This is in keeping with what Neil Gotonda identifies as our nation's commitment to a color-blind ideology.[82] Yet, as Tracey Maclin, Lenese Herbert, Devon Carbado, Andrew Taslitz, and others have noted, race is a relevant consideration when trying to determine the reasonableness of a search or seizure.[83] For example, the test for a seizure is whether the reasonable person in the defendant's shoes would have felt free to leave or terminate the encounter.[84] A young black male who has grown up in South Central Los Angeles knows that if he is stopped by a police officer, he should do whatever the officer says and not talk back unless he wants to kiss the ground. This young man may not feel free to leave or terminate the encounter with the officer, but if the reviewing court believes the average (white) person would have felt free to leave, then the encounter will not be considered a seizure and the young black male will not be able to complain that his Fourth Amendment rights have been violated.

---

[78] *Id.*

[79] Thompson, *supra* note 76, at 964.

[80] *Id.* at 966.

[81] *See* United States v. Drayton, 536 U.S. 194 (2002); Florida v. Bostick, 501 U.S. 429 (1991); Tennessee v. Garner, 471 U.S. 1 (1985); *see also* Tracey Maclin, *Race and the Fourth Amendment*, 51 VAND. L. REV. 333, 339-40 (1998) ("The majority opinion [in *Garner*] did not even acknowledge that Edward Garner, who was shot in the back of the head by a Memphis officer . . . was a skinny, unarmed black teenager."); Janice Nadler, *No Need to Shout: Bus Sweeps and the Psychology of Coercion*, 2002 SUP. CT. REV. 153, 157 (noting that Christopher Drayton and Clifton Brown, the defendants in *United States v. Drayton*, were two young African American men); Carbado, *supra* note 70, at 977 ("Nowhere in Justice O'Connor's opinion does she entertain the possibility that Bostick may have been targeted because he is black. In fact, Justice O'Connor does not even mention Bostick's race.").

[82] Neil Gotanda, *A Critique of "Our Constitution Is Color-Blind,"* 44 STAN. L. REV. 1 (1991).

[83] Lenese C. Herbert, *Bete Noire: How Race-Based Policing Threatens National Security*, 9 MICH. J. RACE & L. 149 (2003) (critiquing the Court's colorblind Fourth Amendment jurisprudence in *Terry v. Ohio*, *Whren v. United States*, and *Illinois v. Wardlow*); Carbado, *supra* note 70, at 977-88 (critiquing Justice O'Connor's colorblind perspective reflected in *Florida v. Bostick*); Maclin, *Race and the Fourth Amendment*, *supra* note 81, at 370-75 (arguing that since the Court allows a consideration of race when it benefits law enforcement, the Court should allow minority defendants to provide evidence of racial targeting as part of the reasonableness inquiry, which is a totality of the circumstances inquiry); Andrew E. Taslitz, *Stories of Fourth Amendment Disrespect: From Elian to Internment*, 70 FORDHAM L. REV. 2257, 2283 (2002) (arguing that in order to have a more "respect-based Fourth Amendment Jurisprudence" the

It may be less easy for some to see the relevance of race and ethnicity to reasonableness in the search context, but the racial profiling literature suggests the importance of race in this context as well.[85] While police officers may not consciously discriminate against black and brown suspects, implicit bias may color their perceptions of who looks and acts suspiciously, and thus who to stop, question, and search.[86] Moreover, because police tend to focus their crime-fighting efforts in poor, high crime neighborhoods, which tend to be populated by poor minority and immigrant communities, poor black and brown individuals are more likely than other individuals to find themselves being stopped and searched.[87]

---

subjective racial motives of the searching officer must be taken into account when determining whether the police action was reasonable).

[84] United States v. Mendenhall, 446 U.S. 544, 559-60 (1980).

[85] DAVID A. HARRIS, PROFILES IN INJUSTICE: WHY RACIAL PROFILING CANNOT WORK (2002); Angela J. Davis, *Race, Cops, and Traffic Stops*, 51 U. MIAMI L. REV. 425 (1997); David A. Harris, *"Driving While Black" and All Other Traffic Offenses: The Supreme Court and Pretextual Traffic Stops*, 87 J. CRIM. L. & CRIMINOLOGY 544 (1997); David A. Sklansky, *Traffic Stops, Minority Motorists, and the Future of the Fourth Amendment*, 1997 SUP. CT. REV. 271; *see also* Sharon L. Davies, *Profiling Terror*, 1 OHIO ST. J. CRIM. L. 45 (2003) (discussing the post 9/11 arguments in support of ethnic profiling).

[86] L. Song Richardson, *Arrest Efficiency and the Fourth Amendment*, 95 MINN. L. REV. 2035, 2039 (2011) ("[E]ven when officers are not intentionally engaged in conscious racist profiling, implicit biases can lead to a lower threshold for finding identical behavior suspicious when engaged in by blacks than by whites.").

[87] *See* Lenese C. Herbert, *Can't You See What I'm Saying? Making Expressive Conduct a Crime In High-Crime Areas*, 9 GEO. J. ON POVERTY L. & POL'Y 135, 137 (2002).

Numerous studies demonstrate that individuals tend to perceive blacks, particularly young black males, as threatening or aggressive. In one early study, subjects observed a purportedly live (actually bogus) dialogue between two men discussing whether an electrical engineer should stick with his present job at a modest but adequate salary or take a new job offering considerably more pay but no long-term security.[88] The argument quickly heats up and results in one of the men shoving the other.[89] At this point, subjects were asked to characterize the behavior of the man who shoved the other man.[90] Sixty-nine percent of the subjects saw the shove as violent when both men were black.[91] In contrast, when both men were white, only thirteen percent of the subjects found that the same behavior was violent.[92] When the man shoving was black and the man being shoved was white, seventy-five percent saw the shove as aggressive.[93] When the man doing the shoving was white and the man being shoved was black, only seventeen percent saw the shove as aggressive.[94]

The available research also shows a tendency to equate blackness with criminality.[95] A 2002 study tested subjects on their ability to accurately assess danger from individuals holding various objects.[96] Researchers developed a simplistic videogame that presented a series of background and target images.[97] Ten African American and ten white young men were recruited on college campuses to pose as targets.[98] Each target appeared in the game four times—twice with a gun and twice without a gun, with a different object and in a different pose each time.[99] To play the game, subjects needed to decide as quickly as possible whether the target was holding a gun or not.[100] If the target was holding a gun, the subject was supposed to shoot him by pushing a button labeled *shoot* on the right side of a button box.[101] If the target was holding some object other than a gun, the subject was told to press a button labeled *don't shoot* on the left side of the button box.[102] A correct hit, i.e., correctly shooting a target with a gun, earned ten points; and a correct rejection, i.e., refraining from shooting a target with an object other than a gun, earned five points.[103] A false alarm, i.e., shooting a target holding an object other than a gun, resulted in a penalty of minus twenty points; a miss, i.e., not shooting a target holding a gun, resulted in a penalty of forty points.[104] This was to replicate the "payoff matrix" experienced by police officers on the street "where shooting an innocent suspect is a terrible mistake (as in the case of Amadou Diallo), but where the stronger motivation is presumably to avoid misidentifying an armed and hostile target, which could result in the officer's death."[105]

---

[88] Birt L. Duncan, *Differential Social Perception and Attribution of Intergroup Violence: Testing the Lower Limits of Stereotyping of Blacks*, 34 J. PERSONALITY & SOC. PSYCHOL. 590, 593 (1976) (testing 104 white undergraduates at the University of California at Irvine).

[89] *Id.*

[90] *Id.*

[91] *Id.* at 595.

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] Justin D. Levinson et al., *Guilty by Implicit Racial Bias: The Guilty/Not Guilty Implicit Association Test*, 8 OHIO ST. J. CRIM. L. 187 (2010) (finding that subjects held implicit associations between blacks and the status of being guilty).

[96] Joshua Correll et al., *The Police Officers Dilemma: Using Ethnicity to Disambiguate Potentially Threatening Individuals*, 83 J. PERSONALITY & SOC. PSYCHOL. 1314 (2002).

[97] *Id.* at 1315.

Researchers found that subjects fired at an armed target more quickly if he was black than if he was white.[106] Subjects were also quicker to refrain from shooting armed white targets than armed black targets.[107] The study thus showed not only that innocent blacks are more likely than innocent whites to be shot, it also showed that individuals are in a more vulnerable position when dealing with armed white individuals than when dealing with armed black individuals because they are slower to recognize that white targets are armed. Shooter bias was evident not only in white subjects, but also in African American subjects.[108]

---

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] *Id.* at 1315-16.

[102] *Id.* at 1316.

[103] *Id.* at 1317.

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.*

Much of the research on implicit bias suggests that when individuals have to make quick, split-second decisions, implicit bias may limit their ability to control for racial bias caused by stereotypes and prejudice.[109] The research also suggests that making race salient can help egalitarian-minded individuals to suppress what would otherwise be automatic stereotype-congruent responses and to act in a more egalitarian manner.[110] This research suggests the possibility that judges, who have more time to deliberate than police officers on the street, might be less prone to the ill-effects of implicit bias. The available research, however, shows that judges, just like other individuals, are influenced by implicit race bias.[111] It also suggests that judges can and do compensate for their own implicit racial bias, at least when race is made salient and the judges are attempting to render racially neutral decisions.[112]

In a 2009 study, Jeff Rachlinski, Sherri Lynn Johnson, Andrew Wistrich, and Chris Guthrie studied the effects of implicit bias on 133 trial judges who were given three hypothetical cases, one involving a juvenile shoplifter, a second involving a juvenile robber, and a third involving a battery.[113] Suspecting "that the judges might respond differently depending upon whether . . . the race of the defendant [was] salient," the researchers did not explicitly identify the race of the defendant in the first two scenarios, but used a subliminal priming mechanism to do so indirectly, while explicitly identifying the defendant as either Caucasian or African American in the third hypothetical.[114]

---

[108] *Id.* at 1324, 1327.

[109] B. Keith Payne, *Weapon Bias: Split-Second Decisions and Unintended Stereotyping*, 15 CURRENT DIRECTIONS IN PSYCHOL. SCI. 287, 288 (2006) (when participants had to make a snap judgment as to whether an object was a gun or a harmless object, they falsely saw a gun more often when primed with a black face than when primed with a white face).

[110] William A. Cunningham et al., *Separable Neural Components in the Processing of Black and White Faces*, 15 PSYCHOL. SCI. 806, 811 (2004) (finding that "unwanted prejudicial responses are most likely to occur under conditions of distraction or cognitive overload, when reflective cognitive processes that might modulate an automatically activated evaluation are otherwise engaged"); Patricia G. Devine, *Stereotypes and Prejudice: Their Automatic and Controlled Components*, 56 J. PERSONALITY & SOC. PSYCHOL. 5, 12, 14 (1989) (finding that when racial stereotypes about blacks were made salient, low-prejudice individuals seemed to consciously mediate their thoughts about blacks and align their thoughts with their egalitarian beliefs, but when race was not made salient, they responded in stereotype-congruent ways). For a fuller description of these and other studies, see Cynthia Lee, *The Gay Panic Defense*, 42 U.C. DAVIS L. REV. 471, 536-49 (2008).

[111] *See* Jeffrey J. Rachlinski et al., *Does Unconscious Racial Bias Affect Trial Judges?*, 84 NOTRE DAME L. REV. 1195 (2009) (finding that judges hold implicit racial biases that can influence their judgment).

[112] *Id.*

Rachlinski found that in the first two experiments where the race of the defendant was not identified explicitly, judges who exhibited a white preference on the Implicit Association Test (IAT) gave harsher sentences to defendants if they had been primed with black associated words rather than neutral words.[115] In other words, judges who had implicit bias in favor of whites were more likely to be harsher in their sentencing of black defendants than in their sentencing of similarly situated white defendants. Judges in the third experiment, where the race of the defendant was identified explicitly, did not judge the white and black defendants differently.[116] Most of the judges in the third experiment reported that they suspected racial bias was being studied, even though the only cue they received was the explicit mention of the defendant's race.[117] This study suggests the usefulness of making race salient —perhaps by defense attorneys calling attention to the possibility of implicit racial bias affecting perceptions of dangerousness, criminality, and threat—when the case involves a black defendant.

The problematic nature of open-ended reasonableness standards has led some feminist scholars to argue in favor of more subjective standards over purportedly neutral objective ones. In the self-defense context, for example, some feminist scholars have argued that battered women who kill their abusers in non-confrontational situations should not be held to the usual reasonable person standard but should be compared to the average battered woman.[118] In the Fourth Amendment context, Dana Raigrodski urges the Court to abandon reasonableness standards altogether.[119]

---

[113] *Id.* at 1211.

[114] *Id.*

[115] *Id.* at 1214-16.

[116] *Id.* at 1219.

[117] *Id.* at 1223-24.

While I agree with the concerns raised by Raigrodski and others, I do not see the Court jettisoning reasonableness as the cornerstone of its Fourth Amendment jurisprudence anytime soon. Moreover, even if it wanted to, it would be difficult for the Court to abandon reasonableness as a requirement for a valid search or seizure. The text of the Fourth Amendment includes an explicit command that searches and seizures not be unreasonable. Rather than abandoning reasonableness, the Court should require more rigorous scrutiny of government claims of Fourth Amendment reasonableness. It should also provide more guidance to lower courts as to when a search ought to be deemed reasonable or unreasonable. Such guidance can minimize problems of inconsistency and arbitrariness. It can also lead to fairer results as possibilities for subconscious bias to influence the decision-making process would be restricted.

IV. THE FUTURE: A HYBRID APPROACH

In other work, I have suggested that the Court should embrace a more rigorous standard of reasonableness review—a standard I call "reasonableness with teeth."[120] Looking outside the criminal procedure arena, I borrow from a small slice of the Court's equal protection jurisprudence and draw lessons from three cases in which the Supreme Court utilized rational basis review to strike down the challenged legislation as unconstitutional. In this Part, I first examine the Supreme Court's

---

[118] *See* CAROLINE A. FORELL & DONNA M. MATTHEWS, A LAW OF HER OWN: THE REASONABLE WOMAN AS A MEASURE OF MAN (2000) (arguing that a reasonable woman standard should be adopted in certain legal contexts); Kit Kinports, *Defending Battered Women's Self-Defense Claims*, 67 OR. L. REV. 393, 415 (1988) (arguing that since courts in self-defense cases consider at least some of the defendant's attributes and circumstances, they should likewise permit an instruction directing the jury to measure the defendant's actions against those of the reasonable battered woman).

[119] Raigrodski, *supra* note 75, at 214-15.

[120] Cynthia Lee, *Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us about the Fourth Amendment*, 100 J. CRIM. L. & CRIMINOLOGY 1403 (2010) [hereinafter Lee, *Package Bombs, Footlockers, and Laptops*].

"rational basis with bite" jurisprudence. Next, I examine possible arguments against importing rational basis with bite into the Fourth Amendment context. I focus my attention here on Richard Worf's use of political process theory to defend judicial deference to the legislature in cases involving suspicionless searches.[121] Finally, I discuss a few ways the Court might implement a more rigorous form of reasonableness review.

Under the Court's equal protection jurisprudence, if a law burdens a fundamental right or targets a suspect class, such as race, alienage, or national origin, the reviewing court must apply strict scrutiny review, striking down the legislation unless it is narrowly tailored to serve a compelling governmental interest.[122] If the legislation discriminates on the basis of gender, the Court will apply heightened or intermediate scrutiny, striking down the legislation if it fails to substantially further an important governmental purpose.[123] If a law does not target a suspect or quasi-suspect class, the Court will uphold the legislation as long as the classification "bears a rational relation to some legitimate end."[124]

In most cases, the level of scrutiny employed predetermines whether the legislation will be struck down as constitutionally infirm or upheld. If strict scrutiny or intermediate scrutiny applies, the legislation will almost always be struck down. As Gerald Gunther put it, strict scrutiny is "'strict' in theory, [but] fatal in fact."[125] On the other hand, if rational basis review is the applicable standard, the legislation will almost always be upheld.[126] The Court applying rational basis review is supposed to defer to the legislature because it is presumed that even improvident or unwise social or economic legislation will eventually be corrected through the democratic process.[127]

---

[121] Richard C. Worf, *The Case for Rational Basis Review of General Suspicionless Searches and Seizures*, 23 TOURO L. REV. 93 (2007) [hereinafter Worf, *The Case for Rational Basis Review*].

[122] City of Cleburne v. Cleburne Living Ctr., 473 U.S. 432, 440 (1985).

[123] Clark v. Jeter, 486 U.S. 456, 461 (1988) (noting that intermediate scrutiny has been applied to discriminatory classifications based on illegitimacy); Miss. Univ. for Women v. Hogan, 458 U.S. 718, 723-24 (1982) (gender classifications subjected to intermediate scrutiny).

[124] Romer v. Evans, 517 U.S. 620, 631 (1996).

[125] Gerald Gunther, *In Search of Evolving Doctrine on a Changing Court: A Model for a Newer Equal Protection*, 86 HARV. L. REV. 1, 8 (1972).

[126] Ashutosh Bhagwat, *Purpose Scrutiny in Constitutional Analysis*, 85 CALIF. L. REV. 297, 304 (1997).

In three rare cases, which Cass Sunstein calls the "*Moreno-Cleburne-Romer* Trilogy,"[128] the Court utilized rational basis review but struck down the legislation in question. What the three cases had in common was that the legislation in question in each case affected a politically unpopular group. The legislation in *Moreno* was aimed at preventing poor, unrelated persons living under one roof from being eligible for food stamps.[129] The ordinance in *Cleburne* made it more difficult for a group home for the mentally disabled to qualify for a zoning permit,[130] and the legislation in *Romer* prohibited any governmental action designed to protect gays and lesbians from discrimination.[131]

Instead of rubber-stamping the legislation in question as it usually does when it applies rational basis review, the Court struck down the challenged enactments in each of these cases on equal protection grounds.[132] The Court went out of its way to note that a desire to harm a politically unpopular group (hippies in *Moreno*, mentally disabled persons in *Cleburne*, and gays and lesbians in *Romer*) is not a legitimate governmental interest. Commentators have called the less-deferential-than-usual rational basis review that was exercised in these cases "rational basis review with a bite."[133]

Borrowing from the Court's "rational basis with bite" jurisprudence, I suggest that courts deciding the validity of a search should conduct a more rigorous inquiry into the overall reasonableness of the search. In other words, the reviewing court should apply reasonableness review *with teeth*. The reviewing court should resist the urge to defer to the government whenever a criminal defendant challenges a search as unconstitutional. It should stop balancing with its thumb on the scale in favor of the government. It should start rigorously questioning whether the challenged governmental action ought to be upheld. It should scrutinize whether the government had good reason for engaging in the challenged action and whether there were good reasons for the government acting without advance judicial authorization.

---

[127] *City of Cleburne*, 473 U.S. at 440.

[128] Cass R. Sunstein, *Leaving Things Undecided*, 110 HARV. L. REV. 4, 59, 61 (1996).

[129] USDA v. Moreno, 413 U.S. 528, 530, 534-35 (1973).

[130] *City of Cleburne*, 473 U.S. at 436-37.

[131] Romer v. Evans, 517 U.S. 620, 624 (1996).

[132] *See* Sunstein, *supra* note 128, at 59-63.

[133] *See, e.g.*, Bhagwat, *supra* note 126, at 327; Gunther, *supra* note 125, at 18-19.

In proposing "reasonableness with teeth," I do not suggest that the Court simply import what it has done in the equal protection context into the Fourth Amendment context. One problem with borrowing from the Court's "rational basis with bite" jurisprudence is that the Court has provided little guidance regarding when "rational basis with bite" is appropriate and virtually no guidance with respect to what "rational basis with bite" means besides heightened judicial scrutiny of the challenged governmental action.[134] Another problem is that the Court applies deferential rational basis review in most equal protection cases and applies non-deferential "rational basis with bite" in only a small minority of cases.[135]

Reasonableness with teeth in the Fourth Amendment context need not replicate these problems. First, factors relevant to whether a search should be deemed reasonable can and should be spelled out in advance—reducing vagueness and lack of guidance concerns. Second, it is unnecessary to limit reasonableness with teeth to cases in which a politically unpopular group has been disadvantaged.[136] Non-deferential reasonableness review should apply in all cases where the validity of a search is at issue, not simply those cases implicating a politically unpopular group. Since the Fourth Amendment requires that all searches and seizures be reasonable, not just those directed at politically unpopular groups, reasonableness is already required for all searches and seizures. The only question is what form reasonableness review ought to take. Nothing in the Fourth Amendment requires that reasonableness review be deferential to the government.[137] Indeed, given the concerns that motivated the Framers to include the Fourth Amendment in the Bill of Rights (the desire to constrain arbitrary and exploratory governmental searches and seizures), a non-deferential standard of review is more appropriate than a deferential, pro-government standard of review.[138]

---

[134] *See* Lee, *Package Bombs, Footlockers, and Laptops*, *supra* note 120, at 1492.

[135] *See* Robert C. Farrell, *Successful Rational Basis Claims in the Supreme Court from the 1971 Term Through* Romer v. Evans, 32 IND. L. REV. 357 (1999).

[136] Arguably, every criminal case in which a search is challenged involves a politically unpopular group, the group of persons identified as criminal defendants. *See* Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; Or, Why Don't Legislatures Give a Damn About the Rights of the Accused?*, 44 SYRACUSE L. REV. 1079 (1993) [hereinafter Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice*] (arguing that legislatures undervalue the rights of criminal defendants); Adam M. Gershowitz, *Imposing a Cap on Capital Punishment*, 72 MO. L. REV. 73, 116-17 (2007) (arguing that the unpopularity of criminal defendants "make[] them the quintessential discrete and insular minority"); Adam M. Gershowitz, *The Invisible Pillar of Gideon*, 80 IND. L.J. 571, 594 (2005) (arguing that criminal defendants are an unpopular group); David A. Sklansky, *Quasi-Affirmative Rights in Constitutional Criminal Procedure*, 88 VA. L. REV. 1229, 1290 (2002) (noting that criminal defendants as a group are "peculiarly powerless to protect themselves through the normal processes of majoritarian democracy"); William J. Stuntz, *Substance,*

I do not suggest that the Court completely abandon all of the doctrines it has carefully established over the years. While I feel several Fourth Amendment doctrines are in desperate need of reform, such as the consent doctrine and the administrative search doctrine, the basic idea behind the warrant preference view

---

Process and the Civil-Criminal Line, 7 J. CONTEMP. LEGAL ISSUES 1, 20-21 (1996) (arguing that criminal suspects as a group find it hard or impossible to protect themselves through the political process). Moreover, the vast majority of criminal defendants are poor and/or black or Latino. Jamie Fellner, *Race, Drugs, and Law Enforcement in the United States*, 20 STAN. L. & POL'Y REV. 257, 257 (2009) (noting strong empirical evidence that "black Americans are disproportionately arrested, convicted, and incarcerated on drug charges"); Erica J. Hashimoto, *Class Matters*, 101 J. CRIM. L. & CRIMINOLOGY 31, 62 (2011) ("[There is] sufficient data to establish that low-income people constitute a disproportionate percentage of criminal defendants."); Cecelia Klingele et al., *Reimaging Criminal Justice*, 2010 WIS. L. REV. 953, 962 (2010) ("Although African Americans comprise less than thirteen percent of the U.S. population, thirty-eight percent of our country's two million prison inmates are black."); Anthony O'Rourke, *The Political Economy of Criminal Procedure Litigation*, 45 GA. L. REV. 721, 734-35 & n.47, 737 (2011) (explaining that "race and class disparities intersect to concentrate the burdens of incarceration among the most socially disadvantaged groups of individuals" with the result that "poor and minority individuals (who . . . constitute the vast majority of criminal defendants)"); William J. Stuntz, *Unequal Justice*, 121 HARV. L. REV. 1969, 1970-71 (2008) ("African Americans constitute 13% of the general population, but nearly half of a record-high prison population.").

[137] *See* Lee, *Package Bombs, Footlockers, and Laptops*, *supra* note 120, at 1492.

[138] *See* Maclin, *The Central Meaning of the Fourth Amendment*, *supra* note 67 (arguing that the central meaning of the Fourth Amendment is distrust of police power and discretion).

—that searches that take place with a search warrant and warrantless searches that fall within an exception to the warrant requirement ought to be presumed reasonable—is sound. Indeed, I believe the wisest course of action is to continue to adhere to the warrant preference view and strengthen the warrant process. Because the Court has clearly indicated this is not the path it intends to pursue, I offer reasonableness with teeth as an improvement on current reasonableness balancing. Instead of simply balancing the government's interests against the individual's interests, a process that in today's post-9/11 world is likely to almost always result in a conclusion that the government's interests outweigh the individual's interests, courts should engage in non-deferential review of the reasonableness of the search or seizure in question.

My focus here is less on *how* non-deferential reasonableness review ought to be implemented than on *why* non-deferential reasonableness review ought to be embraced in light of increasingly popular proposals to shift Fourth Amendment decision making from the province of the judiciary to the province of the legislature. For example, Richard Worf has argued that judges should generally defer to legislative judgments regarding the reasonableness of suspicionless group searches because legislatures are better able than courts to serve democratic interests.[139] Worf relies on political process theory, the idea that when a constitutional provision is ambiguous, "the majoritarian decision[s] of the legislature should . . . be preferred [over] the decisions of unelected and unaccountable judges."[140]

Worf starts by claiming that in the Fourth Amendment arena, "[t]he Court essentially applies strict scrutiny in every case" because it balances de novo and does not defer to legislative judgments.[141] It is difficult to see how Worf can conclude that the Court is applying strict scrutiny when it engages in reasonableness balancing. In most cases, once the Court finds a special need above and beyond the normal need for law enforcement, it concludes that the government's interests outweigh the individual's interests.[142]

---

[139] Worf, *The Case for Rational Basis Review*, *supra* note 121.

[140] *Id.* at 100-01.

[141] *Id.* at 105.

Perhaps the problem is in the way Worf conceives of reasonableness. Worf equates reasonableness in the Fourth Amendment context with cost-effectiveness.[143] He writes, "Reasonableness must, in some sense, mean only cost-effectiveness."[144] I take issue with the proposition that if something is cost-effective, then it must be reasonable. Take, for example, a corporation that manufactures widgets with a defective part. Even if research suggests that a user of this widget stands a one percent chance of being maimed or disfigured, the corporation's board of directors might decide to continue manufacturing the widget after weighing the costs and benefits because it thinks the risk of the defect being discovered is small. Additionally, the board may conclude that even if someone is injured and sues, the cost to settle such a lawsuit will likely be less than the profit the corporation stands to gain from manufacturing the widget without disclosure. Cost-effective? Perhaps. Reasonable? No. Reasonableness in other contexts, such as the self-defense doctrine, is recognized as including a normative component.[145] Reasonableness in the search and seizure context ought to include a normative component as well.

Building on this idea that reasonableness in the Fourth Amendment context means cost-effective, Worf provides five reasons why he thinks legislatures would be better able than courts to decide questions regarding the reasonableness of a suspicionless group search regime. First, he argues that "legislatures have a developed capacity to register the costs and benefits of a practice."[146] Second, legislatures "have better access to the relevant facts."[147] Courts only have the facts of the particular case before them. Legislatures, in contrast, can "seek out facts instead of relying simply on those that interested parties put before them."[148] Third, Worf thinks legislatures have more legitimacy than courts because ordinary people can be involved in setting policies that affect them.[149] Fourth, Worf argues that "legislatures can [better] accommodate local variations in reasonableness."[150] The Supreme Court, in contrast, sets standards of reasonableness that apply nationwide. Fifth, Worf argues that legislatures are better able than courts to adapt to changed circumstances because courts are bound by rules of stare decisis.[151]

---

[142] Illinois v. Lidster, 540 U.S. 419 (2004); Bd. of Educ. v. Earl, 536 U.S. 822 (2002); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995); Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990); Nat'l Treasury Emp. Union v. Von Raab, 489 U.S. 656 (1989); Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602 (1989); Griffin v. Wisconsin, 483 U.S. 868 (1987); New York v. Burger, 482 U.S. 691 (1987); O'Connor v. Ortega, 480 U.S. 709 (1987); New Jersey v. T.L.O., 469 U.S. 325 (1985); United States v. Martinez-Fuerte, 428 U.S. 543 (1976).

[143] Worf, *supra* note 121, at 117.

[144] *Id.*

[145] *See* LEE, MURDER AND THE REASONABLE MAN, *supra* note 2.

[146] Worf, *supra* note 121, at 120.

Worf's arguments are similar to arguments made by my colleague, Orin Kerr, who suggests that legislatures, not courts, ought to be entrusted with protecting citizen privacy interests vis-a-vis new technologies.[152] Kerr provides three reasons why he believes courts should defer to legislatures when it comes to questions regarding the privacy implications of evolving technologies. First, because courts are resolving disputes arising from past events, Fourth Amendment rules tend to lag behind parallel statutory rules and current technologies.[153] Given the way our criminal justice system works, it can take a long time before an issue is resolved by the Supreme Court.[154] The Court generally does not step in until after the circuit courts of appeals have addressed an issue, and usually only to resolve a circuit split. Second, Kerr notes that "[j]udicial rulemaking is limited by strong stare decisis norms that limit the ability of judicial rules to change quickly."[155] Legislatures, in contrast, can respond more quickly to changing facts.[156] Finally, Kerr notes that "[l]egislative rules tend to be the product of a wide range of inputs," whereas judicial rules are the result of "written briefs and oral arguments by [only] two parties."[157]

---

[147] *Id.* at 124.

[148] *Id.* at 125.

[149] *Id.* at 126-27.

[150] *Id.* at 127.

[151] *Id.* at 128-29.

[152] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004).

[153] *Id.* at 868 ("[L]egislatures typically create generally applicable rules ex ante, while courts tend to create rules ex post in a case-by-case fashion").

[154] *Id.* at 868-69.

[155] *Id.* at 871.

Both Worf and Kerr argue that those affected by the searches they discuss (suspicionless group searches in Worf's case and searches involving new technologies in Kerr's case) can adequately protect themselves through the political process.[158] Worf claims that the typical searched or seized group—students subjected to drug testing, people who ride the subway, or drivers who drive on a particular highway—is medium-sized and therefore well positioned to achieve their aims through the political process.[159] He argues that such groups "have numerous members, so they have the economies of scale that individuals lack."[160] He also claims they "are not so large that collective action and free rider problems are [avoided]."[161] Realistically, however, how many people who ride the subway in New York City are going to take the time to try to band together to complain about random subway searches? How would drivers who use a particular route contact other similarly situated drivers so as to lodge a complaint about an objectionable checkpoint? And even if they were successful in organizing like-minded individuals in protesting a particular checkpoint, how likely is it that the legislature would actually listen to them and eliminate the checkpoint after the legislature has weighed the alternatives and made the decision to establish the checkpoint? Not likely.

Kerr makes a similar argument with respect to advances in technology.[162] He notes that the main consumers of new technologies, like the computer and the Internet, are affluent white majorities.[163] Kerr argues that "[s]uch users generally will be able to represent their interests before Congress effectively, resulting in a healthy debate and relatively favorable [outcomes] for balanced legislative rules."[164] While it may be true that affluent whites use computers and the Internet in greater numbers than poor minorities, to date, I have not seen affluent whites banding together to ask Congress to pass legislation curtailing the government's practice of engaging in suspicionless searches of laptops at international airports.[165]

---

[156] *Id.*

[157] *Id.* at 875.

[158] Worf, *The Case for Rational Basis Review*, *supra* note 121; *see also* Kerr, *supra* note 151.

[159] Worf, *The Case for Rational Basis Review*, *supra* note 121, at 132.

[160] *Id.*

[161] *Id.*

[162] Kerr, *supra* note 152, at 887.

[163] *Id.*

The main reason courts should not defer to legislatures when it comes to Fourth Amendment questions rests on institutional competency and separation of powers grounds.[166] The judiciary should not defer to the legislature in matters involving the Fourth Amendment because the judiciary has the primary authority over matters involving constitutional interpretation.[167] This is particularly true in cases affecting the interests of a "discrete and insular minorit[y]."[168] In almost all Fourth Amendment cases, the affected individuals are criminal defendants, individuals who have been charged with a crime, who arguably constitute a "discrete and insular minorit[y]."[169] Because this particular group is an unpopular and disfavored group, it is unlikely to find redress in the majoritarian legislature.[170]

---

[164] *Id.*

[165] Since July of 2008, the Department of Homeland Security has permitted federal agents at the border or its functional equivalent to search and seize laptops and other electronic devices without a warrant and without any individualized suspicion. Ellen Nakashima, *Expanded Powers to Search Travelers at Border Detailed*, WASH. POST, Sept. 23, 2008, at A2 (discussing U.S. CUSTOMS AND BORDER PROTECTION POLICY REGARDING BORDER SEARCH OF INFORMATION (July 16, 2008); U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, DIRECTIVE NO. 7-6.0, BORDER SEARCHES OF DOCUMENTS AND ELECTRONIC MEDIA (July 16, 2008)). In September 2010, the ACLU along with other organizations filed a lawsuit against the Department of Homeland Security, challenging the constitutionality of its laptop policy. Press Release, ACLU, Abidor v. Napolitano: The ACLU Challenges Suspicionless Laptop Border Policy (Mar. 30, 2011), *available at* http://www.aclu.org/free-speech-technology-and-liberty/abidor-v-napolitano.

[166] Fabio Aricla, Jr., *Special Needs and Special Deference: Suspicionless Civil Searches in the Modern Regulatory State*, 56 ADMIN. L. REV. 1223, 1256-57 (2004) (arguing that it is inappropriate to accord *Chevron* style deference to legislatures in the Fourth Amendment context because "neither the legislature nor the executive branch has the power to delegate any portion of the judiciary's constitutional adjudicatory power").

[167] Marbury v. Madison, 5 U.S. 137 (1803).

[168] United States v. Carolene Prods. Co., 304 U.S. 144, 153 n.4 (1938).

[169] *See supra* note 136 and accompanying text.

What might reasonableness with teeth look like in practice? Reasonableness review with teeth could take any number of forms. Without choosing one form over another, I examine a few possibilities here.

First, the current model of open-ended reasonableness balancing could be replaced with Christopher Slobogin's two part proportionality and exigency framework.[171] Slobogin suggests that all searches should first satisfy a proportionality principle.[172] Proportionality, as explained by Slobogin, means the justification for the search must be roughly proportionate to its intrusiveness.[173] If the search in question is extremely intrusive, then the government needs a stronger justification to engage in that search.[174] Slobogin suggests the use of hit rates to measure the strength of the government's justification.[175] Second, under Slobogin's proposed framework, unless there are exigent circumstances, the government must obtain ex ante authorization for the search.[176] Slobogin explains that such advance authorization does not always have to take the form of a warrant based on probable cause issued by a judicial magistrate.[177]

---

[170] Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice*, *supra* note 136.

[171] Christopher Slobogin, *Government Dragnets*, 73 LAW & CONTEMP. PROBS. 107 (2010) [hereinafter Slobogin, *Government Dragnets*]; Christopher Slobogin, *Let's Not Bury* Terry: *A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053 (1998) [hereinafter Slobogin, *Let's Not Bury* Terry]; Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1 (1991) [hereinafter Slobogin, *The World Without a Fourth Amendment*]; SLOBOGIN, PRIVACY AT RISK, *supra* note 16, ch. 2.

[172] SLOBOGIN, PRIVACY AT RISK, *supra* note 16, at 21-22; Slobogin, *Government Dragnets*, *supra* note 171, at 138; Slobogin, *Let's Not Bury* Terry, *supra* note 171, at 1054. Other scholars have suggested that the Court adopt a proportionality principle in its Fourth Amendment jurisprudence, but unlike Slobogin, have argued that the amount of justification required should vary depending on the seriousness of the offense as opposed to the intrusiveness of the government action. *See, e.g.*, Jeffrey Bellin, *Crime Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 IOWA L. REV. 1 (2011) (arguing that Fourth Amendment reasonableness review should include consideration of the seriousness of the crime being investigated such that as the crime increases in severity, the government response can increase in intrusiveness and still be considered reasonable); Colb, *supra* note 66, at 1673-77 (arguing that a more stringent showing of probable cause should be required when the offense being investigated is minor).

[173] SLOBOGIN, PRIVACY AT RISK, *supra* note 16, at 21 ("[The reconceptualization of the Fourth Amendment's] key component can be stated very simply: a search or seizure is reasonable if the strength of its justification is roughly proportionate to the level of intrusion associated with the police action. I call this concept the proportionality principle."); Slobogin, *Government Dragnets*, *supra* note 171, at 138; Slobogin, *Let's Not Bury* Terry, *supra* note 171, at 1054; Slobogin, *The World Without a Fourth Amendment*, *supra* note 171, at 4.

Slobogin's proposed framework makes a lot of sense. Unlike the current reasonableness balancing test, which allows the reviewing court to pick and choose which factors it considers relevant, Slobogin's proportionality principle tells the reviewing court it must focus on intrusiveness and hit rates.[178] Unlike the current model of reasonableness balancing, which encourages the reviewing court to place its thumb on the scale in favor of the government in assessing the government's interests against the individual's interests, Slobogin's proportionality principle looks at hit rates or likelihood of success, not the importance of the asserted governmental interest.[179] Slobogin's proportionality principle also requires the reviewing court to consider the intrusiveness of the government action on the individual or individuals who are subjected to the search.[180] The only problem with Slobogin's proposal is that he would exempt most of the suspicionless group searches, searches he calls "government dragnets," from his proposed framework.[181] In many government dragnet cases, Slobogin would follow Richard Worf's deference to the legislature approach.[182] The reviewing court would be encouraged to simply rubber stamp the government's search regime as long as a legislative body was responsible for creating and implementing it.

---

[174] SLOBOGIN, PRIVACY AT RISK, *supra* note 16, at 38 (explaining, for example, that extremely invasive actions such as "bodily surgery, perusal of private diaries, and prolonged undercover operations . . . should take place only if there is clear and convincing proof that the evidence thereby sought is crucial to the state's case); Slobogin, *Government Dragnets*, *supra* note 171, at 139; Slobogin, *Let's Not Bury* Terry, *supra* note 171, at 1082-84 (explaining a four-tiered approach where the level of intrusiveness dictates the justification required ranging from clear and convincing evidence to probable cause to reasonable suspicion to a relevance standard); Slobogin, *The World Without a Fourth Amendment*, *supra* note 171, at 68 ("[F]or example, the government would generally have to show a higher degree of confidence that a search will be successful when evidence is thought to be in a private home than when it is believed to be in a warehouse or in the 'open fields.'").

[175] SLOBOGIN, PRIVACY AT RISK, *supra* note 16, at 41-42; Slobogin, *Government Dragnets*, *supra* note 171, at 139; Slobogin, *Let's Not Bury* Terry, *supra* note 171, at 1088.

[176] SLOBOGIN, PRIVACY AT RISK, *supra* note 16, at 44 ("[W]hen there is no exigency, ex ante review of the search by some independent official should be preferred—a tenet this book will call the *exigency principle*."); Slobogin, *Government Dragnets*, *supra* note 171, at 141; Slobogin, *The World Without a Fourth Amendment*, *supra* note 171, at 75 (explaining that the exigency principle entails that "whenever some level of justification is required, authorization by a neutral third party should be obtained in all nonexigent situations").

[177] Slobogin, *Government Dragnets*, *supra* note 171, at 141.

[178] *Id.* at 139 ("Under proportionality reasoning, the more intrusive a dragnet program is, the higher its hit rate must be.").

A second way to achieve less deferential reasonableness review is by embracing a multidimensional balancing approach, such as the one proposed by Alexander Reinert.[183] Under Reinert's proposal, courts reviewing the reasonableness of a search should recognize that the "public interest" is multifaceted and includes collective values that are actually in harmony with individual liberties. Reinert identifies two categories of collective interests ignored by the Supreme Court's current jurisprudence: participatory pluralism and efficient administration of the criminal justice system. Reinert explains that when an individual is subjected to a Fourth Amendment intrusion, he may be less likely to participate in civic activities in the future out of fear that he may expose himself to more such intrusions.[184] This is particularly true if the individual feels he was singled out because of his membership in a particular racial or ethnic group.[185] Reinert points to the post-9/11 intrusions on Arab, Muslim, and South Asian communities as an example of how Fourth Amendment intrusions can negatively affect civic participation.[186] He notes that "in the wake of widely held reports of law enforcement tracking and prosecuting donations to particular Islamic charities in this country, civic participation of Muslim communities steeply declined."[187]

---

[179] *Id.* at 140.

[180] *Id.*

[181] *Id.* at 109-10.

[182] *Id.*

[183] Reinert, *supra* note 34.

[184] *Id.* at 1487-89.

[185] *Id.*

[186] *Id.* at 1488.

Reinert identifies a second collective interest that is impinged upon by Fourth Amendment intrusions: the efficient administration of criminal justice.[188] Reinert notes that as the Court has relaxed the justification required for certain kinds of Fourth Amendment intrusions, the likelihood that innocent individuals will be intruded upon increases.[189] For example, the Court's move in *Terry v. Ohio* from requiring probable cause for all seizures of the person to permitting police officers to briefly seize individuals based on reasonable suspicion of criminal activity has resulted in more innocent people being stopped.[190] This creates the potential for hostility against law enforcement and bogs down the criminal justice system.

I agree with Reinert that courts engaging in reasonableness balancing should be open to considering collective harms of the kind he identifies. The problem with his proposal is that it does not adequately respond to two of the problems associated with the current reasonableness balancing test—lack of guidance and overly broad discretion. It simply adds more things for the reviewing court to consider in the overall reasonableness balancing mix.

A third way reasonableness with teeth review might be implemented is through a framework of presumptions. Under such a framework, courts would assess the reasonableness of a search using a hybrid warrant preference-reasonableness approach. As it does under the warrant preference model, the reviewing court would start by asking whether the government agent was acting pursuant to a warrant or an exception to the warrant requirement other than special needs. If so, the court would presume the search was reasonable. If, however, the government agent did not procure a warrant, the reviewing court would need to assess the validity of the search by engaging in a more rigorous form of reasonableness review than is employed today. In other words, the reviewing court would engage in reasonableness review with teeth.

---

[187] *Id.*

[188] *Id.* at 1491.

[189] *Id.* at 1492-93.

[190] *Id.* at 1493-94.

Instead of balancing the government's interests against the individual's interests or looking to framing era common law, the reviewing court would primarily consider three factors. It could consider a fourth factor only if the facts clearly suggested its presence. If the warrantless search did not fall within an established exception to the warrant requirement, the reviewing court would consider these factors to see if any one factor or combination of factors led to a presumption of unreasonableness. If, on the other hand, the warrantless search satisfied the requirements of an established exception to the warrant requirement, then the reviewing court would only be able to override the initial presumption of reasonableness of that search if the court found at least two factors leading to a presumption of unreasonableness.

Under my proposed framework, the reviewing court would first consider the nature and scope of the intrusion. It would ask whether the search was highly intrusive or involved an intrusion into a repository for highly personal or private material or information. If so, the court would apply a presumption of unreasonableness. This first consideration recognizes that privacy is one of the core values protected by the Fourth Amendment.[191]

One might question the wisdom of asking the reviewing court to consider whether the search involved an intrusion on privacy when presumably the court has already decided that the government intruded upon a reasonable expectation of privacy and therefore conducted a search. The court, however, would not be revisiting the reasonable expectation of privacy test. This first inquiry does not ask whether the government intruded upon a reasonable expectation of privacy. Instead, it focuses on the nature and scope of the intrusion, using privacy as a metric. The mere fact that the government has intruded upon a reasonable expectation of privacy merely tells us that the Fourth Amendment is implicated. It does not tell us whether the government violated the Fourth Amendment. The Court has recognized that there are varying degrees of intrusiveness.[192] While I disagree with the Court's assumption that individuals have lessened expectations of privacy in their cars, the fact remains that the Court and many individuals consider the search of a home more intrusive than the search of an automobile in part because the home is a place where very private things are kept and where very private things are said and done.[193] A strip search involving the viewing of private parts is considered more intrusive than a frisk of the outer clothing.[194] Similarly, many would consider the search of a personal computer more intrusive than the search of a cigarette package.[195]

---

[191] Camara v. Municipal Court, 387 U.S. 523, 528 (1967) ("The basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."); Schmerber v. California, 384 U.S. 757, 767 (1966) ("The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusions by the State."); Wolf v. Colorado, 338 U.S. 25, 27 (1949) ("The security of one's privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society.").

---

[192] Atwater v. City of Lago Vista, 532 U.S. 318, 363 (2001) (noting that while both traffic stops and full custodial arrests "are seizures that fall within the ambit of the Fourth Amendment, the latter entails a much greater intrusion on an individual's liberty and privacy interests").

[193] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31 (2001) (noting that "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion" stands at the very core of the Fourth Amendment (internal citations omitted)); California v. Acevedo, 500 U.S. 565, 569 (1991) (noting the distinction made at early common law between the search of a dwelling house and the search of a moving vehicle).

[194] Safford Unified Sch. Dist. #1 v. Redding, 129 S. Ct. 2633, 2641-43 (2009) (distinguishing between the suspicion needed to search a backpack and outer clothes and the suspicion needed to conduct a strip search).

[195] I am not completely comfortable with suggesting that the nature and scope of the intrusion should matter. In previous cases, the Court has refused to draw a distinction between "worthy" and "unworthy" containers, explaining:

> For just as the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion, so also may a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case.

United States v. Ross, 456 U.S. 798, 822 (1982). In prior work, I have supported the Court's refusal to draw a distinction between worthy and unworthy containers. *See* Lee, *Package Bombs, Footlockers, and Laptops, supra* note 120.

Second, the court would ask whether the search was supported by probable cause.[196] If the officer lacked probable cause, the court would apply a presumption of unreasonableness. Many Fourth Amendment scholars wisely argue that probable cause must be a part of any Fourth Amendment reasonableness analysis. Scott Sundby, for example, has stated, "[P]robable cause must be at the center of the Fourth Amendment universe."[197] Similarly, George C. Thomas has argued that except in cases involving searches incident to arrest, police should only be allowed to search for evidence when they have probable cause to believe the search will produce evidence of a crime.[198] Thomas notes that requiring probable cause to make a search avoids the harm of suspicionless searches and the risk that government officials will abuse their power.[199]

---

[196] Much has been written on the subject of probable cause. *See, e.g.*, Bruce A. Antkowiak, *Saving Probable Cause*, 40 SUFFOLK U. L. REV. 569 (2007) (noting how the War on Terror has resulted in the erosion and neglect of probable cause); Sherry F. Colb, *Probabilities in Probable Cause and Beyond: Statistical versus Concrete Harms*, 73 LAW & CONTEMP. PROBS. 69 (2010) (assessing whether there is a legal or moral difference between arresting two people, each based on 50/50 odds of guilt, on the one hand, and arresting two people, one of whom is definitely innocent and the other of whom is definitely guilty, when the officer cannot tell which is innocent and which is guilty); Craig S. Lerner, *The Reasonableness of Probable Cause*, 81 TEX. L. REV. 951 (2003) (arguing for a sliding scale of probable cause that takes into account the gravity of the investigated offense and the intrusiveness of the proposed search as part of the reasonableness framework); Max Minzner, *Putting Probability Back into Probable Cause*, 87 TEX. L. REV. 913 (2009) (arguing that the magistrate should consider the track record of both the individual police officer as well as the officer's unit for establishing probable cause in the past when deciding whether to issue a warrant); Wesley MacNeil Oliver, *The Modern History of Probable Cause*, 78 TENN. L. REV. 377 (2011) (explaining that probable cause in the framing era was merely a pleading requirement, not the evidentiary threshold that it represents today); Andrew E. Taslitz, *What is Probable Cause, and Why Should We Care?: The Costs, Benefits, and Meaning of Individualized Suspicion*, 73 LAW & CONTEMP. PROBS. 145, 145 (2010) (defining probable cause as "having four components: one quantitative (How certain must the police be?), one qualitative (How strong must the supporting data sources be?), one temporal (*When* must police and courts make their judgments?), and one moral (Do the police have 'individualized suspicion'?)"); Arcila, *In the Trenches*, *supra* note 27 (arguing that probable cause during the framing era did not play a central role in Fourth Amendment jurisprudence); Colb, *The Qualitative Dimensions of Fourth Amendment "Reasonableness*," *supra* note 66, at 1673-77 (arguing that if the offense of investigation is a minor offense, a more stringent showing of probable cause should be required and that in cases involving serious governmental intrusions, probable cause alone should not be sufficient to justify a search); Kinports, *Diminishing Probable Cause*, *supra* note 5 (arguing that by using phrases such as "reasonable belief" and "reason to believe" when analyzing probable cause, the Supreme Court is risking indirectly combining the higher standard of probable cause with the lower standard of reasonable suspicion).

[197] Scott E. Sundby, *An Ode to Probable Cause: A Brief Response to Professors Amar and Slobogin*, 72 ST. JOHN'S L. REV. 1133, 1138 (1998).

Probable cause alone, however, should not automatically lead to a finding that the search was reasonable. Under current doctrine, probable cause is all that is needed to search a car.[200] Even if the police have time to get a warrant, they are not required to do so under the automobile exception.[201] Arguably, it is not reasonable to search a car that is not readily mobile without obtaining prior judicial authorization.[202] Under current law, probable cause to believe that a person has committed an offense, even a fine-only offense like a seatbelt violation, is sufficient for an officer to effectuate a custodial arrest of the individual, which in turn gives the officer the ability to search the individual and any containers on the individual.[203] The officer who arrested Gail Atwater had probable cause to believe she had violated the law requiring the wearing of a seatbelt, yet many would dispute the Supreme Court's conclusion that her arrest was reasonable.[204]

Third, the reviewing court would ask whether it was impracticable for the police officer to get a warrant prior to searching. Here, the court would want to consider the danger to the officer or the public and risk to the investigation if the officer had stopped to get a warrant. If stopping to get a warrant would have posed little or no danger to the officer, the public, or the investigation, then the court should apply a presumption of unreasonableness.

---

[198] George C. Thomas III, *Time Travel, Hovercraft, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment*, 80 NOTRE DAME L. REV. 1451, 1459 & 1478 (2005); *see also* Thomas K. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483, 627 (1995) (arguing that individualized suspicion should be a component of Fourth Amendment reasonableness analysis because it "recognizes the historical importance of individualized suspicion to the framers of the Constitution, and it provides needed guidance to courts and governmental officials, avoiding the slippery slope of an unprincipled reasonableness analysis").

[199] Thomas, *supra* note 198, at 1479.

[200] Maryland v. Dyson, 527 U.S. 465, 467 (1999) (holding that probable cause alone satisfies the automobile exception to the Fourth Amendment).

[201] *Id.* at 466-67.

[202] The U.S. Supreme Court, however, has ruled that a car search based solely on probable cause is reasonable even if the car is not mobile. Maryland v. Dyson, 527 U.S. 465 (1999) (reversing a state court decision that held that in order for the automobile exception to apply, there had to be not only probable cause to believe that evidence of a crime was in the automobile, but a separate finding of exigency).

[203] Atwater v. City of Lago Vista, 532 U.S. 318 (2001).

[204] Wayne A. Logan, *Reasonableness as a Rule: A Paean to Justice O'Connor's Dissent in* Atwater v. City of Lago Vista, 79 MISS. L.J. 115 (2009).

As an additional consideration, the reviewing court could ask whether the officer acted in good faith or bad faith. Evidence that the officer was acting in bad faith could also result in a presumption of unreasonableness. Bad faith can be reflected in various ways.[205] If, for example, there is evidence that the officer was using the fact that an individual committed a traffic violation as the justification for a stop when the real reason the officer wanted to stop the individual was because the officer had a mere hunch that the individual was involved in illegal activity, this would be an indication that the officer acted in bad faith. Likewise, any evidence that the officer was motivated by a desire to harass would suggest bad faith. If the officer claimed he entered a home in order to render emergency aid to an injured person within, but there is evidence that the officer was more concerned with whether the occupants of the house were engaged in criminal activity than whether anyone was in need of emergency aid, this would also be an indication of bad faith. If there is any indication that the officer was motivated by race, gender, class, or sexual orientation bias, this would suggest bad faith and result in a presumption of unreasonableness.

Consideration of the subjective intent of the officer, however, runs contrary to current law. The Supreme Court, on many occasions, has said that the good faith or bad faith of the officer is irrelevant to the constitutionality of the police action.[206] The

---

[205] John Burkoff defines bad faith in the search context as occurring "when the police officer who is searching acts entirely and deliberately for reasons that do not constitute a proper legal justification for the search." John M. Burkoff, *Bad Faith Searches*, 57 N.Y.U. L. REV. 70, 101 (1982) (arguing that even if objective reasons exist to support a search, if the officer's sole reason for engaging in the search was an improper reason, the officer's bad faith should render the search unconstitutional).

[206] Kentucky v. King, 131 U.S. 1849, 1859 (2011) (opining that considering whether the police in bad faith intentionally created an exigent circumstance to get around the warrant requirement "is fundamentally inconsistent with our Fourth Amendment jurisprudence" which rejects a subjective approach and asks only whether the action

Court's position on subjective intent is a bit hypocritical. Under current doctrine, the government's purpose in establishing a suspicionless search regime is considered a relevant factor in determining whether there was a special need above and beyond the normal need for law enforcement,[207] but the individual police officer's purpose in stopping or searching an individual is considered irrelevant.[208] In other words, the government's "good" purpose is relevant when it can help the government, but the government's "bad" purpose is irrelevant when considering it might help the defendant.[209]

Defenders of the Court's position might argue it is difficult to prove intent and therefore it is best to stick with objective factors when trying to assess questions of reasonableness. While it may be difficult to discern the subjective intent of the government actor, this does not stop us from requiring proof of intent in other areas of the law. For example, the concept of mens rea is a long-established tradition in substantive criminal law where proof of intent is the general rule and liability without intent is the exception.[210] Moreover, it makes sense to consider the bad faith of government actors when the question is the overall reasonableness of a search. How can a search be considered reasonable if the officer's reason for engaging in the search was to

---

was objectively justified); Brigham City v. Stewart, 547 U.S. 398, 404 (2006) (rejecting argument that reviewing court assessing reasonableness of entry into a home under the emergency aid doctrine ought to consider whether the officers were truly motivated primarily by a desire to save lives and property); Whren v. United States, 517 U.S. 806, 813 (1996) ("Subjective intentions play no role in ordinary, probable-cause Fourth Amendment analysis.").

[207] *See* City of Indianapolis v. Edmond, 531 U.S. 32, 40 (2000) (noting that what distinguishes permissible checkpoints from impermissible checkpoints is their primary purpose).

[208] *Id.*

[209] A distinction might be drawn between programmatic purposes, which is what the Court is assessing in special needs cases, and an individual officer's purpose in engaging in a particular search. In other contexts, however, the Court displays similar bias. For example, the Court requires a defendant challenging his conviction on the ground that the government failed to preserve exculpatory evidence to prove that the police acted in bad faith. Arizona v. Youngblood, 488 U.S. 51 (1988). It does not require the government to prove the police acted in good faith.

[210] Morissette v. United States, 342 U.S. 246, 250 (1952) ("The contention that an injury can amount to a crime only when inflicted by intention is no provincial or transient notion.").

harass? How can a search be considered reasonable if the officer's real reason for suspecting the defendant of criminal activity was the defendant's race?

My framework of presumptions approach marries the warrant preference and reasonableness models of the Fourth Amendment, recognizing that both approaches carry considerable advantages. In requiring prior judicial authorization for a search unless an exception to the warrant requirement applies, the warrant preference model reflects the importance of having a neutral third party assess the lawfulness of governmental action that intrudes upon reasonable expectations of privacy. The reasonableness model, on the other hand, reflects the importance of giving both law enforcement officials and judicial officers broad discretion to decide when a warrantless search is appropriate. My hybrid model recognizes the importance of prior judicial authorization for a search in two ways. First, it allows the reviewing court to presume that searches that take place with a search warrant are reasonable. Second, it ensures that a court reviews the validity of the search at some stage of the process—either pre-search if a warrant is obtained or post-search since all warrantless searches would be subject to reasonableness with teeth review. My hybrid model also recognizes the importance of giving reviewing courts broad discretion. This is why my proposal uses a framework of rebuttable presumptions rather than rigid rules.[211]

My approach differs from the Court's current approach to reasonableness in several respects. First, the current approach to reasonableness is largely a balancing test that weighs the government's interests against the individual's interest.[212] The current approach de-emphasizes the importance of warrants and focuses instead on whether, as a general matter, the challenged governmental action ought to be considered reasonable[213] or whether it was unlawful at common law. [214] My hybrid model of reasonableness, in contrast, recognizes the importance of having a neutral third party assess the appropriateness of the search ex ante. Not only does my hybrid model start by asking whether there was a warrant, it incorporates one of the key components of the warrant process, probable cause, into its inquiry and forces the reviewing court to consider whether the officers could have gotten a warrant.

---

[211] Presumptions are a staple of the Supreme Court's jurisprudence and an important source of guidance to lower courts on a variety of issues. For example, the Court has held that lower courts deciding claims of ineffective assistance of counsel under the Sixth Amendment should presume the competence of the trial attorney. *See* Strickland v. Washington, 466 U.S. 668, 689 (1984) ("[A] court must indulge a strong presumption that counsel's conduct falls within the wide range of reasonable professional assistance . . . ."). It has directed lower courts deciding whether to dismiss an indictment on the ground of selective prosecution to apply a presumption that the prosecutor has not violated equal protection. United States v. Armstrong, 517 U.S. 456, 465 (1996) ("In order to dispel the presumption that a prosecutor has not violated equal protection, a criminal defendant must present 'clear evidence to the contrary.'").

Second, aside from instructing lower courts to look to the common law at the time the Fourth Amendment was adopted, the current approach provides little guidance to lower courts as to what factors they ought to consider when assessing the reasonableness of the search. Under the current approach, if the challenged action was not unlawful at the time of the framing, the reviewing court is supposed to balance the governmental interests against the individual's interests.[215] Balancing, however, is problematic in today's world because it is likely to lead to a finding of reasonableness whenever the government claims a national security interest or an interest in protecting the public. Popular today is the notion that individuals ought to be willing to sacrifice some inconvenience and imposition on their privacy interests in the service of the larger collective good, an idea expressed by Joseph Grano more than twenty-five years ago.[216]

By specifying which factors ought to be considered relevant, my proposed approach provides lower courts with some guidance as to when they should deem a search unreasonable without telling them how they must rule. The presumptions I propose are rebuttable, and the ultimate decision is left with the reviewing court. Moreover, my proposal forces courts to be more transparent about why they think a given search is or is not reasonable.

---

[212] *See supra* note 34.

[213] *See supra* notes 27-46.

[214] *See supra* note 47-51.

[215] *See supra* note 51.

[216] Joseph D. Grano, *Probable Cause and Common Sense: A Reply to the Critics of* Illinois v. Gates, 17 U. MICH. J.L. REFORM 465, 497 (1984) (suggesting the need for a community model under which individuals "who share[] the benefits of community living may legitimately be expected to make reasonable sacrifices on behalf of the community's efforts to solve and control crime").

My proposed framework also recognizes that criminal defendants are a politically powerless group in need of enhanced judicial protection.[217] Just as the Court recognized in footnote four of the *Carolene Products* case that the federal judiciary is uniquely positioned to protect the rights of "discrete and insular minorities,"[218] the current Court should recognize that criminal defendants as a group are unlikely to have their interests protected by the popularly elected legislature or executive.

One might object to my proposal on the ground that it does not resolve problems of ambiguity and overly broad discretion inherent in the current approach but merely pushes back the reasonableness determination to a later time. While I agree that my proposal does not provide a magic bullet formula for determining whether and when a search is reasonable, it provides better assistance to lower courts than the current model by narrowing the list of relevant factors they should consider. The proposed framework not only identifies these factors, it also specifies how these factors should be viewed through a series of presumptions.

Let's think about how my proposed framework would work in practice. Let's say police officer Peter has had several run-ins with an individual named Adam and wants to harass Adam because Adam called him a pig during their last encounter. Peter calls his precinct and asks the clerk to check if there are any outstanding arrest warrants for Adam's arrest. When he receives a negative response, Peter calls the neighboring precinct's clerk and asks the same question despite departmental regulations instructing line officers not to call clerks in other precincts without prior authorization from one's supervisor.[219] This time, the clerk tells him there is an outstanding warrant for Adam's arrest based on his failure to pay three recent parking tickets. Armed with this information, Peter may arrest Adam in public.[220] Once Peter arrests Adam and takes him into custody, Peter may conduct a full search of Adam's person.[221] If Peter finds a smart phone in Adam's jacket pocket, Peter not only may seize the smart phone, he may also search its contents, looking at Adam's text messages, e-mails, Facebook entries, photographs, and even bank account information.

---

[217] *See supra* note 136 and accompanying text.

[218] United States v. Carolene Prods. Co., 304 U.S. 144, 153 n.4 (1938).

[219] This hypothetical is loosely based on the facts in *Herring v. United States*, 555 U.S. 135 (2009). Unlike in *Herring*, the clerk in my hypothetical accurately tells Officer Peter that there is an outstanding warrant for Adam's arrest based on his failure to

Under current law, the warrantless search of Adam's smart phone found on Adam's person would likely be deemed lawful under the search incident to arrest doctrine as long as the arrest was lawful and custodial and the search took place substantially contemporaneously with the arrest.[222] Since there was an outstanding warrant for Adam's arrest, the arrest would be considered lawful. The search was substantially contemporaneous with the arrest, and the smart phone was found on Adam's person. Even if Adam password protected his smart phone, this would not necessarily prevent the officer from hacking into the smart phone or forcing him to reveal the password.[223] An alternate justification supporting the warrantless search of a smart phone found on an

---

pay three parking tickets. In *Herring*, the clerk erroneously reported to the officer that there was an outstanding arrest warrant. *Id.* at 137-38.

[220] United States v. Watson, 423 U.S. 411 (1976).

[221] United States v. Robinson, 414 U.S. 218 (1973) (authorizing full search of the person, including containers found on the person, incident to a lawful, custodial arrest).

[222] *See* United States v. Finley, 477 F.3d 250, 259-60 (5th Cir. 2007) (allowing warrantless viewing of text messages on cell phones seized incident to arrest); United States v. Wurie, 612 F. Supp. 2d 104, 109 (D. Mass. 2009) (noting "trend heavily in favor of finding that the search incident to arrest" doctrine applies to cell phones). *But see* State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009) (rejecting application of the search incident to arrest doctrine to cell phones). Over the past few years, the vast majority of courts that have assessed the constitutionality of police searching of cell phones incident to arrest, have approved of the practice. Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, 96 IOWA L. REV. 1125, 1129 (2011). The Supreme Court has not yet ruled on whether an exception to the search incident to arrest doctrine ought to be recognized for warrantless searches of cell phones found on or near a person who has been arrested and taken into custody. Joshua A. Engel, *Doctrinal Collapse: Smart Phones Cause Courts to Reconsider Fourth Amendment Searches of Electronic Devices*, 41 U. MEM. L. REV. 233, 237 (2010).

[223] Gershowitz, *supra* note 222.

arrestee's person is the exigent circumstances exception.[224] Police may worry that if they wait to search the smart phone, a confederate might remotely wipe the phone of its contents.

Under my proposed framework, the reviewing court would start by asking whether the search took place with a warrant or fell within an established exception to the warrant requirement. Here, even though Peter acted without a search warrant, the search falls within the search incident to arrest exception. Accordingly, the search enjoys a presumption of reasonableness that can be overcome only if the reviewing court finds at least two factors pointing to a presumption of unreasonableness in its review for overall reasonableness. In this review, the court would first consider three factors: (1) the nature and scope of the intrusion, (2) whether the officer had probable cause to believe evidence of a crime would be found in the smart phone, and (3) whether it was impracticable for the officer to get a warrant. If there is clear evidence of bad faith, the reviewing court could also consider the officer's bad faith.

The reviewing court could first find that the search of a smart phone is extremely intrusive given the vast amounts of personal information a smart phone is capable of storing. Second, in this case, it does not appear that the officer had any specific and articulable facts leading him to believe that the smart phone he searched contained any incriminating evidence. Adam was arrested because he had three outstanding parking tickets. It was not likely that Adam's smart phone would yield any further evidence supporting the offense of arrest. Third, it was not impracticable for Peter to have gotten a search warrant to search the smart phone. Once Peter had possession of the smart phone and took Adam in custody, it was unlikely that Adam would be able to destroy any evidence on the smart phone, unless he had access to a computer or could call an accomplice and tell the accomplice to wipe the smart phone. Additionally, Peter's purpose in arresting and searching Adam was to harass Adam for calling him a pig, suggesting bad faith. All of these factors would point to a presumption that the search was unreasonable, overriding the initial presumption of reasonableness, and allowing the court to find the search unconstitutional.

---

[224] As one court noted, "evidence may be lost due to the dynamic nature of the information stored on and deleted from cell phones or pagers." United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1278 (D. Kan. 2007).

One problem with my framework of presumptions approach is that it does not work so well in the case of administrative searches. This is because in most administrative search cases, there is no individualized suspicion or probable cause, suggesting a presumption of unreasonableness, but it is also impracticable to obtain a search warrant in advance, suggesting a presumption of reasonableness. These two factors cancel each other out, leaving the court to consider the nature and scope of the intrusion. The problem here is that just considering the nature and scope of the intrusion without also considering the government's interests may lead to balancing with the thumb on the scale in favor of the individual rather than fair balancing. Moreover, evidence of bad faith will only be present in a limited number of cases. More attention needs to be paid to the question of how to implement less deferential review of administrative searches, but I will leave that question to another day.

CONCLUSION

The Supreme Court has moved away from reading the Fourth Amendment as expressing a preference for warrants to understanding it as requiring only reasonableness, not warrants. The Court today stands at a crossroads. It can completely replace the warrant preference model with the reasonableness model of the Fourth Amendment, as it has already done in a few cases; it can return to a robust embrace of the warrant preference view; or it can recognize the virtues of the warrant preference and the reasonableness models and improve upon both. Because the Court is unlikely to return to a robust embrace of warrants, I argue that the Court should continue its current path of recognizing both models. Instead of extremely deferential pro-government reasonableness balancing, however, I argue that courts should engage in a more stringent form of Fourth Amendment reasonableness review. Courts assessing the reasonableness of a Fourth Amendment search should employ reasonableness review with teeth.

NO MORE CHIPPING AWAY: THE ROBERTS COURT USES AN AXE TO TAKE OUT THE FOURTH AMENDMENT EXCLUSIONARY RULE

Tracey Maclin[*] & *Jennifer Rader*[**]

INTRODUCTION 1184
I. WHAT THE ROBERTS COURT EXCLUSIONARY RULE CASES ARE *REALLY* ABOUT 1186
  A. Davis *Confirms the Direction of the Court* 1189
  B. The Future of Suppression: Why All Eyes Are Rightly on Justice Kennedy 1191
    1. Justice Kennedy's Influence in *James v. Illinois* 1193
    2. Justice Kennedy: Not So "Moderate" on the Exclusionary Rule 1198
II. *HERRING* AND *DAVIS*: YES, THE COURT MEANT WHAT IT SAID 1201
  A. Herring*'s Move Towards Suppression for Only Deliberate and Culpable Conduct* 1201
  B. Davis *Not Only Embraces, but Expands* Herring 1205
  C. What the Court's Good-Faith Exception in Herring *and* Davis *Means for the Future of the Exclusionary Rule* 1207
  D. Justice White's Roadmap for the Roberts Court's Good-Faith Exception 1210
III. BEYOND GOOD-FAITH: APPLYING *HUDSON V. MICHIGAN*'S LOGIC TO BAR SUPPRESSION AS A CATEGORICAL MATTER 1214
  A. Justice Scalia's Three Rationales in Hudson 1214

---

[*] Professor of Law, Boston University School of Law. I want to thank Professor Thomas K. Clancy, Director of the National Center for Justice and the Rule of Law, for inviting me to participate in this symposium.

[**] J.D. Candidate, 2013, Boston University School of Law.

B. Two Different Forms of Attenuation: Traditional and Hudson v. Michigan *Attenuation* 1217
C. Extending Hudson's *Attenuation Logic Beyond the "Knock-and-Announce" Context*................................1219
  1. *Hudson* and the "No Press" Rule..........................1219
  2. *Hudson* and the "Right-to-See-a-Warrant" Rule...1220
  3. *Hudson* and the "No Arbitrary Destruction of Property" Rule..1223
  4. *Hudson* and the "Inventory Search" Rules...........1224
CONCLUSION 1227

INTRODUCTION

This symposium is on the future of Fourth Amendment law. This essay focuses on the Fourth Amendment exclusionary rule, which requires that evidence obtained from an unconstitutional search or seizure be excluded from a criminal prosecution.[1] There was a time when the exclusionary rule or suppression doctrine was considered part and parcel of the amendment.[2] However, the modern Supreme Court no longer sees the rule as anchored by the Fourth Amendment itself. In the mid-1970s, the Burger Court jettisoned the view that the exclusionary rule is a personal right; instead, the Court explained that the rule is a judicially created remedy to deter police violations of the amendment.[3] The Rehnquist and Roberts Courts have emphatically reaffirmed this view of the rule. Thus, the Court envisions the rule in strictly instrumental terms and not in remedial terms the way the Framers thought about remedies for rights violations.[4]

---

[1] There are several different types of constitutional "exclusionary rules" that mandate the suppression of evidence in criminal prosecutions, and they are not identical in nature. This essay discusses exclusion mandated by Fourth Amendment rules. For an excellent and comprehensive discussion of constitutional exclusionary rules, see JAMES J. TOMKOVICZ, CONSTITUTIONAL EXCLUSION: THE RULES, RIGHTS, AND REMEDIES THAT STRIKE THE BALANCE BETWEEN FREEDOM AND ORDER (2011).

[2] *See* Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 (1920) ("The essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court but that it shall not be used at all."); Weeks v. United States, 232 U.S. 383, 393 (1914) ("If [documents illegally acquired can be] used in evidence against a citizen accused of an offense, the protection of the Fourth Amendment declaring his right to be secure against such searches and seizures is of no value, and, so far as those thus placed are concerned, might as well be stricken from the Constitution."); Thomas S. Schrock & Robert C. Welsh, *Up from* Calandra*: The Exclusionary Rule as a Constitutional Requirement*, 59 MINN. L. REV. 251, 282 (1974) (stating that *Weeks* "recognized a personal fourth amendment right to exclusion").

Since the mid-twentieth century, the exclusionary rule has been a controversial topic—both on and off the Court. After he retired from the Court, Potter Stewart compared its development in the Court to "a roller coaster track constructed while the roller coaster sped along."[5] In a little-noticed opinion in 1979, then-Justice Rehnquist claimed that "one of the central themes" presented in the sweep of the Court's exclusionary rule jurisprudence, which, according to Rehnquist, began in 1914, "has been a continuing re-evaluation of past assumptions."[6] In that opinion, Rehnquist thought a reassessment of the exclusionary rule was overdue, and he urged his colleagues to consider whether, and to what extent, the rule should be retained.[7] This Article proposes a "reassessment" as well; it provides an evaluation of the Roberts Court's intentions for the exclusionary rule. The Article, therefore, departs slightly from the theme of the symposium because it considers the current status of the exclusionary rule under the Roberts Court,[8] as well as what the future holds for the rule.

---

[3] *See, e.g.*, Stone v. Powell, 428 U.S. 465, 486 (1976); United States v. Calandra, 414 U.S. 338, 348 (1974).

[4] *See, e.g.*, Albert W. Alschuler, Herring v. United States*: A Minnow or a Shark?*, 7 OHIO ST. J. CRIM. L. 463, 501-07, 510-11 (2009) ("In accordance with the view that a right implies a remedy, the courts of the Founding generation held officers personally liable in damages for every wrongful search and seizure. Yet today the Supreme Court threatens to leave most violations of the Fourth Amendment without any remedy, not even on paper."). For an interesting defense of the exclusionary rule from an originalist's perspective, see Roger Roots, *The Originalist Case for the Fourth Amendment Exclusionary Rule*, 45 GONZ. L. REV. 1, 4 (2010) (contending that "the Fourth Amendment exclusionary rule is soundly based in the original understandings of the Constitution and the practices of the Founding period").

[5] Potter Stewart, *The Road to* Mapp v. Ohio *and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 COLUM. L. REV. 1365, 1366 (1983). Stewart also remarks that the rule suppresses evidence that would not have been available if the police had "complied with the commands of the fourth amendment in the first place." *Id.* at 1392. Professor Susan Bandes rightly observes that "the controversial nature of the remedy has much to do with the controversial nature of the underlying right." Susan A. Bandes, *The Roberts Court and the Future of the Exclusionary Rule*, AM. CONST. SOC'Y FOR L. & POL'Y, Apr. 2009, at 1, *available at* http://www.acslaw.org/files/Bandes%20Issue%20Brief.pdf.

[6] California v. Minjares, 443 U.S. 916, 922 (1979) (Rehnquist, J., dissenting).

[7] *Id.* at 928.

Despite Justice Kennedy's 2006 declaration that "the continued operation of the exclusionary rule, as settled and defined by our precedents, is not in doubt,"[9] this Article demonstrates why this is not the case. Kennedy's statement is noteworthy and has been accorded substantial weight primarily because it was made at a time when it was thought that four Justices (Chief Justice Roberts, and Justices Scalia, Thomas, and Alito) were prepared to announce the demise of the exclusionary rule. Part I provides the background for the Court's recent suppression rulings and Kennedy's 2006 statement. Part II then considers the substance and worth of Kennedy's statement as it pertains to *Davis v. United States*[10] and *Herring v. United States*,[11] the Court's most recent rulings on the good-faith exception to the exclusionary rule. Part III considers the meaning of Kennedy's statement in light of the attenuation rule announced in *Hudson v. Michigan*, which imposed a significant restriction on suppression as a remedy to deter Fourth Amendment violations.[12]

I. WHAT THE ROBERTS COURT EXCLUSIONARY RULE CASES ARE *REALLY* ABOUT

The mainstream press reports on and reacts to the Court's latest rulings on the Fourth Amendment exclusionary rule with a subtle uniformity. In theory, the exclusionary rule requires that evidence acquired from an unconstitutional search or seizure be excluded from a criminal prosecution. In reality, the Court has created many exceptions to the rule that have greatly reduced its applicability and impact. Nonetheless, much of the public assumes the rule prevents the conviction of guilty defendants. Ironically, twenty-one years have elapsed since the Court upheld application of the exclusionary rule in a search and seizure case; Justices Brennan and Marshall were still on the Court![13] Since then, the Court has decided six exclusionary rule cases, ruling for the government in every case.[14]

---

[8] Professor Tom Clancy contends that when it comes to search and seizure law, "it is now Scalia's Court." Thomas K. Clancy, *The Irrelevancy of the Fourth Amendment in the Roberts Court*, 85 CHI.-KENT L. REV. 191, 195 (2010). According to Clancy, "Scalia stands alone on the current Court. He has vision, force, and perseverance. It is his Court when it comes to the Fourth Amendment and it is his goal to make it irrelevant." *Id.* at 196.

[9] Hudson v. Michigan, 547 U.S. 586, 603 (2006) (Kennedy, J., concurring in part and concurring in the judgment). For a discerning analysis of Kennedy's concurrence in *Hudson*, see James J. Tomkovicz, Hudson v. Michigan *and the Future of Fourth Amendment Exclusion*, 93 IOWA L. REV. 1819, 1832-33, 1848-49, 1880-81 (2008) [hereinafter Tomkovicz, *the Future*].

[10] 131 S. Ct. 2419 (2011).

[11] 555 U.S. 135 (2009).

[12] 547 U.S. 586 (2006).

When the Court announces a new ruling addressing the exclusionary rule, as it did recently in *Davis v. United States*,[15] the reaction in the press is somewhat predictable. Inevitably the press reports that the rule has lost favor with the Justices, or the Court has created "another" exception to the rule that makes it harder for criminal defendants to suppress evidence obtained pursuant to illegal searches. But these same reports typically contain an observation that the Court seems unwilling to abolish the rule.

Lyle Denniston's post concerning *Davis* on SCOTUSblog is representative of this phenomenon. Denniston, a veteran and respected Supreme Court reporter, wrote that the exclusionary rule "is fading further as a restraint on police evidence-gathering,"[16] and that the result in *Davis* indicates that a solid majority of the Court "is deeply skeptical of the rule [and] appears to be adding new Justices."[17] But Denniston's column also noted that a majority of the Court "does not yet seem ready to cast aside altogether the 'exclusionary rule.'"[18] Two years earlier, after the

---

[13] *See, e.g.*, James v. Illinois, 493 U.S. 307 (1990).

[14] *See Davis*, 131 S. Ct. 2419; *Herring*, 555 U.S. 135; *Hudson*, 547 U.S. 586; Pa. Bd. of Prob. & Parole v. Scott, 524 U.S. 357 (1998); Arizona v. Evans, 514 U.S. 1 (1995); New York v. Harris, 495 U.S. 14 (1990).

[15] 131 S. Ct. 2419.

[16] Of course, the exclusionary rule does not "restrain" police evidence-gathering techniques—the Fourth Amendment does. The exclusionary rule, when it applies, merely makes the Fourth Amendment relevant.

[17] Lyle Denniston, *Opinion Analysis: The Fading "Exclusionary Rule,"* SCOTUSBLOG (June 25, 2011, 8:58 AM), http://www.scotusblog.com/?p=122938.

[18] *Id.*; *see also* Craig M. Bradley, *Red* Herring *or the Death of the Exclusionary Rule?*, 45 TRIAL 52 (2009) [hereinafter Bradley, *Red* Herring] (describing the result in *Herring* as "another, fairly minor, chip out of the exclusionary rule"); Craig M. Bradley, *Mixed Messages on the Exclusionary Rule,* 42 TRIAL 56 (2006) [hereinafter Bradley, *Mixed Messages*] ("Four justices in the majority—Antonin Scalia (the author), Clarence Thomas, John Roberts, and Samuel Alito—appear ready to eviscerate the exclusionary

Court decided *Herring v. United States*,[19] Adam Liptak, who covers the Supreme Court for the *New York Times*, adopted a more solemn view of the status of the exclusionary rule. Interestingly, Liptak's story on *Herring* opened with the revelation that as an attorney in the Reagan White House in 1983, John Roberts "was hard at work on what he called in a memorandum 'the campaign to amend or abolish the exclusionary rule.'"[20] Roberts, of course, would later become Chief Justice of the United States and the author of *Herring*. Liptak's story noted that *Herring* was significant because it was the first time the Court had permitted the admission of illegally obtained evidence when "all that was involved was isolated [police] carelessness."[21] Liptak also wrote that the result in *Herring* "suggested that the exclusionary rule itself might be at risk."[22] Liptak later observed that "the fate of the rule seems to turn on the views" of Justice Kennedy, who, according to Liptak, "has sent mixed signals" on whether the rule should be retained.[23]

While press coverage of the Court's exclusionary rule cases is factually accurate, something is missing in these reports. What is not mentioned is a thoughtful awareness of the Court's intentions

---

principle. The rule was saved from this fate in *Hudson* only by a confusing (or confused) concurring opinion written by Justice Anthony Kennedy."); Linda Greenhouse, *Justices Will Hear Case on Evidence Suppression*, N.Y. TIMES, Feb. 20, 2008, at A15, *available at* http://www.nytimes.com/2008/02/20/us/20scotus.html (finding that the Justices "have made no secret of their desire to carve more exceptions out of the . . . exclusionary rule" and "Justice Antonin Scalia's majority opinion [in *Hudson*] *appeared* written to solicit further challenges to the rule's application" (emphasis added)); Christine Dowling, *A Massive But Dubious Look at California's Death Penalty*, CRIME & CONSEQUENCES BLOG (June 20, 2011, 1:29 PM), http://www.crimeandconsequences.com/crimblog/ 2011/06/news-scan-964.html (noting briefly that Alito's opinion in *Davis* represents "further paring back applicability of the exclusionary rule"); Adam Liptak, *U.S. Is Alone in Rejecting All Evidence if Police Err*, N.Y. TIMES, July 19, 2008, http://www.nytimes.com/2008/07/19/us/19exclude.html ("The Supreme Court has in recent years whittled away at the exclusionary rule by limiting its applicability and creating exceptions to it. . . . [In] *Hudson v. Michigan*, Justice Scalia *seemed* to say that the exclusionary rule had outlived its original purpose." (emphasis added)).

[19] 555 U.S. 135 (2009).

[20] Adam Liptak, *Justices Step Closer to Repeal of Evidence Ruling*, N.Y. TIMES, Jan. 31, 2009, at A1, *available at* http://www.nytimes.com/2009/01/31/washington/ 31scotus.html.

[21] *Id.*

[22] *Id.*

[23] *Id.*

for the exclusionary rule. Put simply, what is not being discussed is what these cases are *really* all about. Reporters, of course, are often not trained as lawyers and are not experts on constitutional criminal procedure. But members of the Court know their colleagues' intentions better than the press. Thus, it was somewhat odd to read portions of Justice Breyer's dissent in *Davis* questioning whether his colleagues had contemplated the full extent of their ruling's ramifications.

A. Davis *Confirms the Direction of the Court*

At issue in *Davis* was whether the good-faith exception to the exclusionary rule should extend to a case where police conduct a search relying on binding judicial precedent that is subsequently overruled. By a seven-to-two vote, the Court ruled that the exclusionary rule does not apply in this context.[24] *Davis* provided a ringing endorsement of *Herring*'s edict that to trigger the rule police behavior must be sufficiently deliberate that suppression can meaningfully deter it and sufficiently culpable that such deterrence is "worth the price paid by the justice system."[25] As will be explained below, the result and reasoning in *Davis* was predictable and consistent with the goal of either abolishing or confining the exclusionary rule to egregious police misconduct. In his dissent, Justice Breyer questioned whether the Court was serious about the consequences of its reasoning:

> [*I*]*f* the Court means what it now says, *if* it would place determinative weight upon the culpability of an individual officer's conduct, and *if* it would apply the exclusionary rule only where a Fourth Amendment violation was "deliberate, reckless, or grossly negligent," then the "good faith" exception will swallow the exclusionary rule.[26]

Perhaps Breyer's comments were an effort to put the best spin on a decision that reaffirms what was said in *Herring*, which Professor Wayne LaFave, "America's preeminent authority on the law of the Fourth Amendment,"[27] describes as "flat-out wrong."[28] Or, perhaps Breyer's comments were offered in the hope that one or more of the Justices in the *Davis* majority would come to regret his or her decision to join the *Davis* opinion.[29] In any event, unlike Justice Breyer, we have no doubt that the *Davis* majority, as well as the *Herring* majority, meant what it said when it asserted the exclusionary rule is applicable only where a Fourth Amendment violation was "deliberate, reckless, or grossly negligent."[30] Put another way, rather than offer another warning of the possible *future* demise of the exclusionary rule, this Article emphasizes a different point: The revolution is over and the opponents of the exclusionary rule have won (Though we concede that some "mop-up" work may be required to convince the lower courts that the Court meant what it said in *Davis* and *Herring*, namely, that exclusion is unwarranted in all cases where police reasonably believed their conduct complied with the law).

---

[24] Davis v. United States, 131 S. Ct. 2419, 2434 (2011).

[25] *Id.* at 2428 (quoting Herring v. United States, 555 U.S. 135, 144 (2009)).

[26] *Id.* at 2439 (Breyer, J., dissenting) (emphasis added).

Although some may think the result in *Davis* is simply more "chipping away" at the exclusionary rule and not cause for alarm, we disagree. The rationale of *Davis* confirms that the Court intends to limit application of the rule to deliberate, bad-faith, or recurring Fourth Amendment violations. But there is more. The reasoning and logic of *Hudson v. Michigan*,[31] another Roberts Court ruling, provides the Court an additional jurisprudential tool to bar exclusion even when police deliberately violate the Fourth Amendment. *Hudson* held violations of the Fourth Amendment knock-and-announce rule never require the exclusion of evidence. The tone and language of Justice Scalia's opinion in *Hudson* exhibits contempt and opposition toward suppression.[32] *Hudson*'s holding was based, in part, on a novel interpretation of the attenuation rule, which is another exception to the exclusionary rule. As will be explained in Part III, the new vision of attenuation adopted in *Hudson* easily applies to Fourth Amendment protections besides the knock-and-announce rule, which means additional injunctions against the suppression doctrine.

---

[27] Albert W. Alschuler, *The Exclusionary Rule and Causation:* Hudson v. Michigan *and Its Ancestors*, 93 IOWA L. REV. 1741, 1744 (2008) [hereinafter Alschuler, *Exclusionary Rule*].

[28] Wayne R. LaFave, *The Smell of* Herring*: A Critique of the Supreme Court's Latest Assault on the Exclusionary Rule*, 99 J. CRIM. L. & CRIMINOLOGY 757, 758 (2009).

[29] Although it is far too early to make any firm judgments about Justice Kagan's views, liberals should worry that she joined Justice Alito's opinion in *Davis* without qualification.

[30] *Herring*, 555 U.S. at 144.

[31] 547 U.S. 586 (2006).

[32] Clancy, *supra* note 8, at 202 (stating that at its "most fundamental level," the result in *Hudson* "called into question the future of the exclusionary rule," and that abolition of the rule "is Scalia's clear aim; he has planted the seeds in *Hudson* and

B. The Future of Suppression: Why All Eyes Are Rightly on Justice Kennedy

Despite the rulings in *Hudson*, *Herring*, and *Davis*, some judges and legal commentators may still insist that the exclusionary rule is alive and well, although somewhat staggered. This view is undoubtedly fueled by the comments of Justice Kennedy, the crucial swing vote on the Roberts Court. In *Hudson*, Kennedy provided the fifth vote and concurred in the three key parts of Scalia's opinion. Regarding the suppression doctrine, Kennedy said: "[T]he continued operation of the exclusionary rule, as settled and defined by our precedents, is not in doubt."[33] Deciphering what Kennedy meant "turns out to be a challenge."[34] Indeed, a skeptic might "wonder why, if the current operation of the exclusionary rule were *not* in doubt, such a declaration would be required."[35] After reading *Hudson*, a few things came to mind: First, Justice Scalia had lined up the votes to repeal the rule, but Kennedy decided against that move and was signaling his support for the rule—at least for now. On the other hand, why would Kennedy join an opinion that laid the seeds for the destruction of

---

needs one more vote to reap the harvest"). Professor Tomkovicz agrees that *Hudson* can be read as a sign that the Court is ready to abolish the rule. *See* Tomkovicz, *the Future*, *supra* note 9, at 1841-47 (explaining that when *Hudson* is broadly read, it "foreshadows and anticipates outright abolition" of the exclusionary rule). However, Tomkovicz believes that is not the best way to interpret *Hudson*—"at least for the present." *Id.* at 1847-49.

[33] *Hudson*, 547 U.S. at 603 (Kennedy, J., concurring in part and concurring in judgment).

[34] Sharon L. Davies & Anna B. Scanlon, Katz *in the Age of* Hudson v. Michigan*: Some Thoughts on "Suppression as a Last Resort*,*"* 41 U.C. DAVIS L. REV. 1035, 1066 (2008).

[35] Donald Dripps, *The Fourth Amendment, The Exclusionary Rule, and the Roberts Court: Normative and Empirical Dimensions of the Over-Deterrence Hypothesis*, 85 CHI.-KENT L. REV. 209, 235 (2010).

the rule?[36] Perhaps Kennedy got "cold feet" after reading Scalia's draft in *Hudson* and was unwilling to go along. Alternatively, perhaps Kennedy had not decided what to do about the rule. A concurring opinion would permit Kennedy to join the result in *Hudson*, which moved the Court closer to abolishing the rule. But it would also allow him more time to think about repealing the rule outright.

Justice Kennedy's votes to join the majority opinions in *Herring* and *Davis* have caused us to reconsider his support for the rule and his claim that the rule is still operative. After these decisions, what type of police conduct triggers the exclusionary rule? And what is the meaning and scope of the rule under the logic of *Hudson* and *Herring*? Besides Kennedy's comment in *Hudson*, there are additional reasons to focus on Kennedy's votes and views as a window into the Court's intentions for the rule.

First, and most obviously, Kennedy is currently the pivotal swing vote on the Court.[37] Professor Albert Alschuler, perhaps tongue-in-cheek, has described Kennedy as "the second most powerful man in America."[38] His votes obviously matter in suppression cases. In *Hudson*, Kennedy provided the crucial fifth vote for the result, and he joined Scalia's novel analysis on the attenuation exception to the exclusionary rule, but refused to join another part of Scalia's opinion. In *Herring*, Kennedy joined the majority, probably again providing the crucial fifth vote. More importantly, Kennedy joined Chief Justice Roberts's opinion in *Herring* without qualification, including the crucial declarations limiting the applicability of the exclusionary rule to deliberate, reckless, or grossly negligent police violations. These assertions in *Herring*—what Professor Alschuler calls the "'big blast' statements"[39]—were unprecedented and controversial,[40] and thus, one might have thought in light of his comment in *Hudson* about preserving the exclusionary rule, Kennedy would have distanced himself from this reasoning.[41]

---

[36] David A. Moran, *The End of the Exclusionary Rule, Among Other Things: The Roberts Court Takes on the Fourth Amendment*, CATO SUP. CT. REV. 283, 308 (2006) ("If he really believes in the continuing vitality of the exclusionary rule, it is an absolute mystery to me why he would cast the crucial fifth vote for an opinion that openly declared war on the exclusionary rule."); Davies & Scanlon, *supra* note 34, at 1068 (noting that Kennedy's "cautionary language" in *Hudson* may mean he is unwilling to provide the fifth vote to repeal the exclusionary rule, yet "Kennedy's willingness to align himself with the most wide-reaching points" in Scalia's opinion "leaves this unclear").

[37] Adam Liptak, *A Significant Term, with Bigger Cases Ahead*, N.Y. TIMES, June 29, 2011, at A12, *available at* http://www.nytimes.com/2011/06/29/us/29scotus.html (reporting that during the 2011 Supreme Court Term, twelve of the fourteen closely divided five-to-four cases were split between the four liberal Justices and four conservative Justices, with "Justice . . . Kennedy casting the decisive vote"); Adam Liptak, *Roberts Court Shifts Right, Tipped by Kennedy*, N.Y. TIMES, July 1, 2009, at A1, *available at* http://www.nytimes.com/2009/07/01/us/01scotus.html (Liptak observes that during the 2009 term Justice Kennedy was in the majority for eighteen of the twenty-three cases where the Justices split five-to-four: "[I]n 16 [of these decisions], all four members of the court's liberal wing were on one side and all four of its conservatives were on the other. And in between them was Justice Kennedy, the most powerful jurist in America.").

[38] Alschuler, *supra* note 4, at 476. Alschuler's description differs from another description of Kennedy. *See* JEFFREY TOOBIN, THE NINE: INSIDE THE SECRET WORLD OF THE SUPREME COURT 199 (2007) (reporting that James Dobson, the founder and

1. Justice Kennedy's Influence in *James v. Illinois*

In addition to being the crucial fifth vote, there is evidence that not only is Kennedy willing to stand alone in opposing extension of the exclusionary rule, but that he is also able to influence like-minded Justices to change their votes in order to restrict application of the rule. According to Justice Brennan's private papers, in *James v. Illinois*, Kennedy's dissent convinced Justices O'Connor and Scalia to change their vote in that case. *James* addressed whether the impeachment exception to the exclusionary rule, which allows prosecutors to use illegally acquired evidence to impeach a defendant who takes the stand, extends to *all* defense witnesses.[42]

In late August 1982, Chicago police detectives suspected fifteen-year-old Darryl James was involved in the murder and

---

director of Focus on the Family, described Kennedy as "the most dangerous man in America").

[39] Alschuler, *supra* note 4, at 472.

[40] LaFave, *supra* note 28, at 760-70.

[41] Alschuler, *supra* note 4, at 476 ("As the indispensable fifth vote, Kennedy probably had the bargaining power to excise the 'big blast' statements from Chief Justice Roberts's opinion if he wished to do so. He certainly could have disassociated himself from these statements in a concurring opinion."); *see also* Bradley, *Red* Herring, *supra* note 18 (observing that it "was a mistake for Kennedy, if he wishes to preserve the exclusionary rule in its present form as he declared in *Hudson*, to go along with the four conservatives in [*Herring*]").

[42] James v. Illinois, 493 U.S. 307 (1990).

shooting of two teenagers. Witnesses to the shooting told police that the shooter had "reddish," straight hair. These same witnesses also said that they had seen James several weeks earlier at a parade, and James's hair was "reddish" and straight.[43] The day after the shooting, detectives found James at his mother's beauty parlor sitting under a hair dryer. When he emerged, his hair was black and curly. After arresting James, the detectives questioned him about his prior hair color. James told the detectives that the previous day his hair had been reddish brown, long, and combed straight back. He also told the police that he had changed his hair color and style on the day of his arrest "in order to change his appearance."[44]

After James was indicted for murder and attempted murder, the trial court ruled that James's statements to the detectives were inadmissible because they were the fruit of an arrest without probable cause.[45] Although James did not testify at the trial, the defense called a family friend, Jewell Henderson, who testified that she had taken James to register for high school on the day of the shooting, and his hair was black and curly on that day.[46] The prosecutor was allowed to impeach Henderson's testimony by introducing James's statements to the police.[47] During closing arguments, the prosecutor told the jury that the State's evidence contained an admission by the defendant that he changed the color of his hair. James was convicted of murder and attempted murder.[48] The Illinois Supreme Court upheld the convictions, ruling that in order to prevent defendants from engaging in perjury "by proxy," the impeachment exception extended to defense witnesses.[49]

At the conference discussion in *James*, only Chief Justice Rehnquist was clearly committed to affirming James's conviction.[50] All the remaining Justices, including O'Connor and Scalia, voted to reverse the conviction. Rehnquist appeared to concede that the ruling below expanded the impeachment exception beyond the Court's prior rulings. Rehnquist also acknowledged that the challenged evidence "is not impeachment but rebuttal."[51] Nonetheless, Rehnquist voted to affirm on the "ground that the exclusionary rule must give way to truth seeking."[52] O'Connor told her colleagues that an affirmance "would encourage improper police conduct."[53] Scalia said that unless the Court was "going to discard the exclusionary rule," he would vote to reverse.[54] Kennedy signaled "he was on the fence,"[55] but ultimately voted to reverse.[56] Thus, the conference vote was eight-to-one for reversal.

---

[43] *Id.* at 310.

[44] *Id.* at 309 (internal quotation marks omitted).

[45] *Id.* at 309-10.

[46] *Id.* at 310.

[47] *Id.*

[48] *Id.* at 311.

[49] People v. James, 528 N.E.2d 723, 730-31 (Ill. 1988), *rev'd sub nom.* James v. Illinois, 493 U.S. 307 (1990).

Justice Brennan assigned *James* to himself, and his first draft closely resembled the final published opinion. He stated his concern that expanding the impeachment to encompass the testimony of all defense witnesses "likely would chill some defendants from presenting their best defense—and sometimes any defense at all—through the testimony of others."[57] Brennan wrote this potential "chilling" effect changed the balance of values that informed the Court's earlier impeachment rulings. While the Court's prior cases recognized that defendants were not permitted to exploit tainted evidence as a shield for perjury, Brennan explained: "[I]t seems no more appropriate for the State to brandish such evidence as a sword with which to dissuade defendants from presenting a meaningful defense through other witnesses."[58]

---

[50] William J. Brennan, Jr., Case Histories 68-69 (Oct. Term, 1989) [hereinafter Case Histories] (on file with the Library of Congress, Manuscript Division, The William J. Brennan Papers, Box II 8, Folder 5).

[51] William J. Brennan, Jr., Brennan's Conference Notes, James v. Illinois (Oct. 6, 1989) (on file with the Library of Congress, Manuscript Division, The William J. Brennan Papers, Box I 859, Folder 4).

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] Case Histories, *supra* note 50.

[56] Harry A. Blackmun, Blackmun's Conference Notes, James v. Illinois (Oct. 6, 1989) (on file with the Library of Congress, Manuscript Division, The Harry A. Blackmun Papers, Box 553).

[57] William J. Brennan, Jr., 1st Draft James v. Illinois 6 (Nov. 2, 1989) (on file with the Library of Congress, Manuscript Division, The Harry A. Blackmun Papers, Box 553).

Brennan also wrote an expanded impeachment exception would undermine the deterrent effects of exclusion. Authorizing the impeachment of defense witnesses was appreciably different than impeachment of defendants for at least two reasons: First, enlarging the impeachment exception would multiply the occasions on which tainted evidence could be used because defense witnesses outnumber testifying defendants. Second, the possession of tainted evidence gives the prosecution leverage not only to deter perjury, but it will "also deter defendants from calling witnesses in the first place, thereby keeping from the jury much probative exculpatory evidence."[59]

After Brennan's first draft was circulated, Justices White, Marshall, Blackmun, and Stevens soon joined the opinion. "For a while, it even appeared that the Chief might switch his vote and join as well." Rehnquist had told his law clerk "to tinker with a draft dissent but said that he wasn't sure he would circulate anything."[60]

In the meantime, Kennedy wrote Brennan a letter stating that "it seems to me that reversal here requires a rule far more sweeping than I had thought at Conference."[61] Kennedy also thought that the state's position would not undermine the purpose of exclusion because he told Brennan that permitting "rebuttal of the false testimony here need not lower the level of deterrence."[62] Kennedy, whose vote to affirm at the conference was shaky, informed Brennan that he would dissent.[63] Kennedy, according to Brennan's records, "was convinced after a strong lobbying from one of his clerks to write a dissent himself."[64] The first draft that Kennedy circulated dismissed Brennan's fears that permitting the use of tainted evidence would encourage future lawless behavior by the police. Kennedy pointed out that similar fears had been raised and rejected in prior cases.[65] This concern—encouraging police misconduct—was the basis for O'Connor's vote at conference. In addition, Kennedy argued that any gain in deterrence achieved by excluding the evidence was "marginal."[66]

---

[58] *Id.* at 8.

[59] *Id.* at 9.

[60] Case Histories, *supra* note 50.

[61] Letter from Justice Kennedy to Justice Brennan (Nov. 21, 1989) (on file with the Library of Congress, The Harry A. Blackmun Papers, Box 553).

[62] *Id.*

[63] *Id.*

[64] Case Histories, *supra* note 50.

Within three hours of receiving Kennedy's draft, Rehnquist and O'Connor joined it.[67] The next day, O'Connor wrote Brennan to explain that she found Kennedy's dissent "persuasive" and thus was shifting her conference vote.[68] After *James* was announced, Brennan's private papers recalled that O'Connor found Kennedy's dissent "'persuasive' (though it merely relied on the same arguments she had herself rejected at Conference)."[69] Two weeks after Kennedy's dissent circulated, Scalia joined and switched his conference vote.[70] Despite the defections of O'Connor and Scalia, Brennan still had five votes and his final opinion rejected an enlargement of the impeachment exception to the exclusionary rule.

In the mid-1970s,[71] and then again in *United States v. Leon*, Justice Brennan complained that the Court was poised to abolish the exclusionary rule.[72] Brennan had a different reaction after *James* was announced. He believed the result in *James* "casts into some doubt the frequent suggestion that the Court is on the verge of overruling *Mapp v. Ohio* and jettisoning the exclusionary rule altogether."[73] For Brennan, the lesson learned in *James* was that Justice White, "the most ardent foe of the rule through his proposed 'good faith' exception, is still the key to preserving the rule against being gutted by attacks along other fronts."[74]

---

[65] Anthony M. Kennedy, 1st Draft James v. Illinois 6 (Nov. 21, 1989) (on file with the Library of Congress, Manuscript Division, The William J. Brennan Papers, Box 859, Folder 5).

[66] *Id.* at 7.

[67] Case Histories, *supra* note 50.

[68] Letter from Justice O'Connor to Justice Brennan (Nov. 22, 1989) (on file with the Library of Congress, Manuscript Division, The William J. Brennan Papers, Box 859, Folder 5).

[69] Case Histories, *supra* note 50.

[70] Letter from Justice Scalia to Justice Brennan (Dec. 7, 1989) (on file with the Library of Congress, Manuscript Division, The William J. Brennan Papers, Box 859, Folder 5).

[71] *See, e.g.*, United States v. Calandra, 414 U.S. 338, 365 (1974) (Brennan, J., dissenting).

[72] United States v. Leon, 468 U.S. 897, 929, 959 (1984) (Brennan, J., dissenting).

[73] Case Histories, *supra* note 50.

Certainly, White's support was essential for preventing an enlargement of the impeachment exception to the exclusionary rule. But another lesson learned from *James* was that Justice Kennedy was an opponent of the exclusionary rule. To be sure, Kennedy's dissent in *James* did not call for repealing the rule, so the depth of his hostility to exclusion could not be judged by a single opinion. However, *James* did reveal that Kennedy wanted to restrict the rule, knowing that a new exception would impact future prosecutions involving defense witnesses and provide additional incentives for police to violate the constitutional rights of criminal suspects in order to obtain incriminating statements.[75] In *James*, Kennedy stood ready to limit exclusion even when like-minded, conservative Justices were initially unwilling to approve a broad, new exception to the rule.

2. Justice Kennedy: Not So "Moderate" on the Exclusionary Rule

Justice Kennedy is often characterized as a "moderate" member of the Court's conservative majority.[76] His votes in a 1992 Pennsylvania abortion case[77] and in a 2003 case invalidating Texas's criminal sodomy law[78] have led the public to perceive Kennedy as a different type of conservative than, say, Scalia and Thomas, or Chief Justice Roberts. But his voting record as a Justice (as opposed to his comment in *Hudson*) indisputably indicates that he is very much opposed to the exclusionary rule. In contrast to other so-called "moderate" Justices who have sat on the Court in recent years, Kennedy has *never* voted to impose the Fourth Amendment exclusionary rule. By comparison, Justices O'Connor and Souter, neither of whom was a fan of the exclusionary rule, did vote to impose the rule at least one time. O'Connor voted for the defendant in *Illinois v. Krull*[79] and *Murray v. United States,*[80] while Souter voted for the defendant in *Pennsylvania Board of Probation & Parole v. Scott.*[81] According to the *New York Times*, O'Connor was also prepared to vote for the defendant in *Hudson*, but she resigned before the Court decided the case.[82] And in a case that was initially argued in the 1983 Term but decided on different grounds a year later, O'Connor wrote an unpublished opinion in which she dissented from the majority's decision that the exclusionary rule does not apply in juvenile delinquency proceedings to bar the admission of evidence obtained from an illegal search by a school official.[83]

---

[74] *Id.*

[75] Note this was shortly before the time when evidence surfaced that California law enforcement agencies were instructing officers that it was permissible to continue questioning suspects who have invoked their *Miranda* rights. *See* Charles D. Weisselberg, *Saving* Miranda, 84 CORNELL L. REV. 109, 132-40 (1998); *id.* at 134 (describing a California training manual that tells instructors voluntary statements obtained from *Miranda* violations can be used to impeach a defendant at trial; as a basis for obtaining physical evidence; and for other investigative purposes, including locating contraband, identifying co-suspects, and locating witnesses).

[76] *See* Bradley, *Red* Herring, *supra* note 18 (describing Kennedy as a "judicial moderate").

[77] Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833 (1992).

[78] Lawrence v. Texas, 539 U.S. 558 (2003). In *Lawrence*, Kennedy authored the majority opinion.

Finally, as a judge on the Ninth Circuit, Kennedy sat on the appellate panel that decided *United States v. Leon*,[84] the progenitor of the good-faith exception that the Roberts Court has transformed and expanded. Kennedy dissented from the ruling ordering the exclusion of evidence obtained pursuant to an invalid search warrant. Like the other judges on the panel, Judge Kennedy declined to discuss a good-faith exception to the exclusionary rule. The closing paragraph of his short dissent, however, took a side-swipe at the exclusionary rule when he observed: "Whatever the merits of the exclusionary rule, its rigidities become compounded unacceptably when courts presume innocent conduct when the only common sense explanation for it is on-going criminal activity."[85]

---

[79] 480 U.S. 340 (1987).

[80] 487 U.S. 533 (1988). In *Murray*, Justice O'Connor joined Justice Marshall's dissent.

[81] 524 U.S. 357 (1998).

[82] *See* Linda Greenhouse, *Court Limits Protection Against Improper Entry*, N.Y. TIMES, June 16, 2006, at A28, *available at* http://www.nytimes.com/2006/06/16/washington/16scotus.html; Charles Lane, *Court Eases "No Knock" Search Ban; Illegally Collected Evidence Allowed*, WASH. POST, June 16, 2006, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/15/AR2006061500730.html; *see also* David A. Moran, *Waiting for the Other Shoe:* Hudson *and the Precarious State of* Mapp, 93 IOWA L. REV. 1725, 1730-31 (2008). O'Connor participated when *Hudson* was originally argued on January 9, 2006. *Id.* at 1730. Her resignation was effective upon the nomination and confirmation of her successor, Samuel Alito, who took his seat on January 31, 2006. *Id.* at 1731. On April 19, 2006, the Court ordered re-argument in *Hudson*, which suggested that the Court was evenly split after O'Connor's resignation. *Id. Hudson* was reargued on May 18, 2006 and decided nearly a month later, this time with Alito providing the fifth vote to affirm Hudson's conviction. *Id.*

[83] Sandra Day O'Connor, Dissent, 1st Draft New Jersey v. T.L.O. (June 12, 1984) (on file with the Library of Congress, Manuscript Division, The Harry A. Blackmun Papers, Box 414).

[84] 468 U.S. 897 (1984).

In sum, Justice Kennedy has been a key player on the Court in restricting the applicability and scope of the exclusionary rule. Without his votes, the opinions in *Hudson* and *Herring* would be very different. Thus, Court-watchers and legal scholars rightly focus on Kennedy because they believe his position will determine the future of the Fourth Amendment's exclusionary rule.[86] While Kennedy's influence and votes have been crucial, it is a mistake to think that the Court remains unsure about the future of the rule. Five Justices have already made their move, although they are not yet marching in lockstep together. Kennedy's statement in *Hudson* on the continued viability of the rule tends to mislead rather than inform readers about the Roberts Court objectives for the rule. Professor Craig Bradley takes the view that a majority of the Court has decided "that the exclusionary rule must be reconsidered."[87] This Article contends that the Roberts Court has already made its intentions known. If outright repeal is unattainable, then the goal is continued prohibition on suppression as a remedy for entire categories of cases, as done for knock-and-announce cases in *Hudson*, and application of the rule only in cases of culpable police misconduct.

---

[85] United States v. Leon, No. 82-1093, 1983 WL 486883, at *3 (9th Cir. Jan. 19, 1983) (Kennedy, J., dissenting).

[86] In a comprehensive and perceptive article on *Hudson v. Michigan*, Professor Tomkovicz offers the view that Justice Kennedy has carefully positioned himself on the exclusionary rule: "It seems fair to say that Justice Kennedy concurred in the [*Hudson*] majority's language and reasoning insofar as they addressed suppression for knock-and-announce violations. He made it clear, however, that he was not participating in any exclusionary rule revolution that might be seen in *Hudson*'s undercurrents." Tomkovicz, *the Future*, *supra* note 9, at 1849; *see also id.* at 1886 (noting that Kennedy's "unavoidable declaration of allegiance to the exclusionary rule . . . indicates that [abolition of the rule] is not imminent"). Professor Tomkovicz's analysis was provided *before* the results in *Herring* and *Davis*.

[87] Craig M. Bradley, *Reconceiving the Fourth Amendment and the Exclusionary Rule*, 73 LAW & CONTEMP. PROBS. 211, 217 (2010), *available at* http://scholarship.law.duke.edu/lcp/vol73/iss3/6/; *see also id.* at 212 (noting that the Court is "dissatisfied with the mandatory aspect of the *Mapp* rule," and that in *Hudson* and *Herring*, the "Court has indicated that the rule should be changed but has stopped short of mandating a broad alteration").

The next two Sections of this Article ponder the Court's most recent exclusionary rule decisions. Specifically, Part II considers what *Herring* and *Davis* tell us about the Roberts Court intentions for the suppression doctrine. Part III considers a specific section of *Hudson v. Michigan* and what it means for the continued operation of the exclusionary rule. Unlike Justice Kennedy, based on our reading of these cases, we think the "continued operation" of the exclusionary rule is very much in doubt.

II. *HERRING* AND *DAVIS*: YES, THE COURT MEANT WHAT IT SAID

Davis v. United States provides convincing evidence that the broad language in *Herring v. United States* on the applicability of the exclusionary was not obiter dicta, but instead was meant to be the core of *Herring*.[88] In order to understand the significance of *Davis*, a description of the reasoning and result in *Herring* is helpful.

A. Herring*'s Move Towards Suppression for Only Deliberate and Culpable Conduct*

While Bennie Dean Herring was checking on his impounded vehicle at the Coffee County, Alabama sheriff's office, sheriff's deputy, Mark Anderson, who was aware of Herring's less-than-perfect background, requested that the Coffee County warrant clerk run a warrant check on Herring.[89] When the warrant search came back negative, Anderson had the warrant clerk call neighboring Dale County to see if there were any outstanding warrants for Herring. The warrant clerk for Dale County reported that there was an outstanding arrest warrant for Herring. This information was relayed to Anderson, who then arrested Herring as he was driving away from the impoundment lot. A search of

---

[88] *See* Alschuler, *supra* note 4, at 474 ("[*Herring*'s] 'big blast' statements look more like *ratio decidendi* (or the Court's 'reason for deciding' as it did) than like *obiter dicta* (or things 'said by the way.') . . . [*Herring*'s big blast] statements appeared as part of a sustained argument." (footnotes omitted)).

[89] Herring v. United States, 555 U.S. 135, 137 (2009).

Herring's person and vehicle incident to arrest revealed narcotics and a weapon.[90] Ten to fifteen minutes later, officials learned that the warrant listed in the Dale County database should not have been there; the warrant had been recalled five months earlier. A negligent employee of the sheriff's office should have removed the warrant.[91] Herring's arrest was illegal.[92]

Although Herring's arrest violated the Fourth Amendment, the evidence discovered incident to his arrest was admitted at his federal narcotics prosecution under the good-faith exception. The lower courts ruled that suppression would serve no deterrent purpose. The officers who arrested Herring were innocent of wrongdoing; the failure to update the computer records was negligent, not a deliberate or tactical decision.[93]

After losing his argument for exclusion in the lower federal courts, Herring appealed to the Supreme Court. Chief Justice Roberts's opinion for a five-to-four majority has been the subject of considerable scrutiny and controversy. While some scholars have interpreted *Herring* narrowly,[94] it is not obvious why Roberts's opinion should be read that way. To be sure, the issue confronting the Court was the one left unresolved in *Arizona v. Evans*,[95] namely, whether the exclusionary rule applies to suppress evidence obtained from an illegal arrest that was prompted by errors in police recordkeeping. But Roberts's opening paragraph suggests that his logic and holding apply beyond the specific facts of the case. Roberts asks: "What if an officer reasonably believes there is an outstanding arrest warrant, but that belief turns out to be wrong because of a negligent bookkeeping error by another police employee?"[96] The Chief Justice provides the following answer: Exclusion of evidence obtained from an illegal arrest is not a mechanical reaction to a Fourth Amendment violation. Rather, "the question turns on the culpability of the police and the potential of exclusion to deter wrongful police conduct. Here the error was the result of isolated negligence attenuated from the arrest. We hold that in these circumstances . . . [exclusion is not appropriate]."[97] Of course, the error in *Herring* involved negligence by a police employee in *another county*, but Roberts's framing of the issue suggested that error by an officer in the same police department should not result in exclusion either.[98]

---

[90] *Id.*

[91] *Id.* at 138.

[92] *Id.*

[93] United States v. Herring, 492 F.3d 1212, 1218 (11th Cir. 2007) *aff'd sub nom.* Herring v. United States, 555 U.S. 135 (2009).

[94] Professor Orin Kerr has written that "*Herring* is a minor case. . . . I think it's a narrow and interstitial decision, not one that is rocking the boat. In particular, I don't see it as suggesting a general good faith exception for police conduct. Such a position would be an extraordinary shift in Fourth Amendment law that would effectively overrule a ton of cases. . . . The decision was quite narrow." Orin Kerr, *Responding to Tom Goldstein on* Herring, VOLOKH CONSPIRACY (Jan. 14, 2009, 2:38 PM), http://volokh.com/posts/1231961926.shtml; *see also* Matthew J. Franck, *Hyperventilating About the Exclusionary Rule*, NAT'L REV. ONLINE (Feb. 16, 2009, 11:21 AM), http://www.nationalreview.com/bench-memos/50452/hyperventilating-about-exclusionary-rule/matthew-j-franck# (describing *Herring* as "really pretty ordinary, and simply applies a principle established . . . in *United States v. Leon*," 468 U.S. 897 (1984), and "there's no sign that the Roberts Court has lost its interest in maintaining" the exclusionary rule).

[95] 514 U.S. 1 (1995).

Professors LaFave and Alschuler have already provided detailed and compelling critiques of Roberts's opinion.[99] We agree with much of their analysis and criticism of *Herring*. Our emphasis is on *Herring*'s statements regarding the type of police conduct that justifies exclusion as a remedy. Specifically, *Herring* stated: "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system."[100] Relying on prior cases, *Herring* asserted: "[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence."[101] Roberts then noted that Deputy Anderson's illegal arrest of Herring did "not rise to that level."[102]

---

[96] *Herring*, 555 U.S. at 136-37.

[97] *Id.* at 137.

[98] Alschuler, *supra* note 4, at 471 ("Roberts asked about the significance of a negligent error by *any* officer other than the one who conducted the search. His opinion implied that even negligence by another officer in the same police agency might be regarded as 'attenuated.'").

[99] *See* Alschuler, *supra* note 4; LaFave, *supra* note 28; *see also* Jennifer E. Laurin, *Trawling for* Herring*: Lessons in Doctrinal Borrowing and Convergence*, 111 COLUM. L. REV. 670, 679-88 (2011) (explaining the reasoning of *Herring* is a significant departure from the Court's prior cases).

[100] *Herring*, 555 U.S. at 144.

[101] *Id.*

[102] *Id.*

A few points about this language should be highlighted. First, it is a mistake to interpret this part of the opinion as dicta. Roberts's description of the level of police culpability necessary to trigger exclusion was stated without qualification. More importantly, this language does not mention "attenuation." Unlike the unexplained references to "attenuation" in other parts of his opinion, the discussion on the need for culpable police conduct to trigger the exclusionary rule appears as part of a "sustained argument."[103] Furthermore, no ruling prior to *Herring* had asserted or even implied that suppression turns on deliberate or grossly negligent police conduct.[104]

Second, it is also a mistake to think that this language from *Herring* will not be cited by the Court when future defendants seek application of the exclusionary rule to ordinary Fourth Amendment violations. To be sure, the "holding" of *Herring* appeared to be bound by the facts. But the opening paragraph of *Herring*, which frames the issue before the Court, suggests that the Chief Justice sees the case as one involving a broader concern beyond the specific facts of the case. If the Chief Justice truly intended a narrow reading of *Herring*, he certainly knew how to write an opinion that would convey to the lower courts that *Herring*'s holding and reasoning were confined to negligent recordkeeping cases. If *Herring* was simply deciding the issue left open in *Arizona v. Evans*, the "big blast" statements were unnecessary to decide the case. It borders on the naïve to think these statements were heedlessly included in the opinion. Rather, the statements were a purposeful addition, as the Roberts Court intends to restrict the exclusionary rule to instances of culpable police behavior.

---

[103] Alschuler, *supra* note 4, at 474.

[104] Alschuler, *supra* note 4, at 488-89 ("No decision prior to *Herring* . . . had suggested or implied that the exclusionary rule should be limited [to culpable police misconduct]. . . . *Herring*'s 'big blast' statements would preclude exclusion even when an officer was not 'objectively reasonable' as long as he was not grossly negligent. Declaring that this standard had been 'laid out in our cases' took chutzpa."); LaFave, *supra* note 28, at 763-68.

B. Davis *Not Only Embraces, but Expands* Herring

Notwithstanding the language on culpable police conduct, erudite scholars rejected the claim that *Herring* was cause for alarm.[105] Justice Alito's opinion in *Davis*, however, indicates that six (and maybe seven) of the current Justices read *Herring* the way we read *Herring*. As noted above, *Davis* addressed whether the exclusionary rule applies when police perform a search in reliance on "binding [judicial] precedent" that is later overruled.[106] *Davis* involved a police search of a car that was lawful at the time of the search, but that was later overruled by the Court while Davis's appeal was pending. When *Davis* arrived at the Court, few thought that Davis had any chance of winning because police reasonably relied on existing law to perform the search. Although all agreed that the search violated the Fourth Amendment, excluding the evidence found from the now-illegal search would serve no deterrent purpose because the officer was neither culpable nor did anything wrong when performing the search. As far as the good-faith exception went, the facts in *Davis* appeared to be on all fours with *Herring* and the Court's previous good-faith cases.[107]

Indeed, Justice Alito held that because exclusion "would do nothing to deter police misconduct" and would impose a high cost to "both the truth and the public safety" the rule does not apply in this context.[108] His opinion explains, relying on *Herring*, that the deterrence benefits of suppression vary with the culpability of the challenged police misconduct: "When the police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights, the deterrent value of exclusion is *strong* and *tends* to outweigh the resulting costs."[109] On the other hand, Alito also elaborates, in line with *Herring*'s focus on culpable police conduct, that when police search or seize "with an objectively 'reasonable good-faith belief' that their conduct is lawful,"[110] or when their unconstitutional behavior "involves only simple, 'isolated' negligence,"[111] deterrence "loses much of its force," and exclusion is not required.[112]

---

[105] *See, e.g.*, Bradley, *Red* Herring, *supra* note 18 (observing that *Herring* "is only a slight change from *Arizona v. Evans*," and that *Herring* "represents another, fairly minor, chip out of the exclusionary rule since most illegal searches will not be attenuated from the error that caused them"). But Bradley did caution that if four of the Justices "get their way, the major pillar upholding Fourth (and Fifth) Amendment rights, will collapse." *Id.*

[106] Davis v. United States, 131 S. Ct. 2419, 2434 (2011).

[107] At first glance, *Davis* might qualify "as a 'no-brainer.'" *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.3 at 21 (4th ed. Supp. 2011-2012). But as Fourth Amendment scholars know, the Court's rulings in this area often require close scrutiny. According to Professor LaFave, "some questions exist with respect to either the result or the majority's reasoning [in *Davis*] that might give one pause." *Id.* Moreover, the result in *Davis* raises significant disincentives for future defendants to challenge search and seizure practices that might result in the creation of new Fourth Amendment law. *See* Orin Kerr, *Good Faith, New Law, and the Scope of the Exclusionary Rule*, 99 GEO. L.J. 1077 (2011).

[108] *Davis*, 131 S. Ct. at 2423-24.

Significantly, *Davis* expands *Herring*, a point recognized by Justice Breyer's dissent.[113] Recall that *Herring*'s "holding" suggested that exclusion is not required in circumstances where the constitutional offense "was the result of isolated negligence *attenuated* from the arrest."[114] Commentators and lower courts that interpreted *Herring* narrowly believed that the attenuation element would contain *Herring*'s impact and prevent its logic from applying to garden-variety Fourth Amendment violations.[115]

---

[109] *Id.* at 2427 (emphasis added) (quoting Herring v. United States, 555 U.S. 135, 144 (2009)). Notice that *Davis* is unwilling to categorically state that when police are culpable, exclusion *is* required. Alito will only say that such conduct provides a "strong" reason to exclude and that exclusion "tends" to outweigh the costs to society.

[110] *Id.* (quoting United States v. Leon, 468 U.S. 897, 909 (1984)).

[111] *Id.* at 2427-28 (quoting *Herring*, 555 U.S. at 137).

[112] *Id.* at 2428 (quoting *Leon*, 468 U.S. at 919).

[113] *Id.* at 2439-40 (Breyer, J., dissenting).

[114] *Herring*, 555 U.S. at 137 (emphasis added).

[115] *See, e.g.*, United States v. Green, Criminal No. 1:08 CR 0041, 2009 WL 230890, at *10 (M.D. Pa. Jan. 30, 2009) (granting the suppression motion following an officer's illegal search and explaining that "the Supreme Court clearly restricted the reach of *Herring's* limitation on the exclusionary rule to police misconduct that is 'attenuated' from the arrest. Unlike the case at bar, *Herring* involved a computer error by police that was remote in both time and location from the unlawful arrest."); State v. Handy, 18 A.3d 179, 187-88 (N.J. 2011) (affirming the suppression motion and concluding that although the police officer reasonably relied on a mistake by a dispatcher, the conduct of the dispatcher was not sufficiently attenuated from the arrest to trigger the good-faith exception in *Herring*); State v. Hess, 785 N.W.2d 568, 579 (Wis. 2010) (explaining that the Supreme Court "held that the police conduct in *Herring* did not warrant exclusion because it 'was the result of isolated negligence attenuated from the arrest,'" and holding that the good-faith exception to the exclusionary rule did not apply to a civil bench warrant that was invalid when issued) (quoting *Herring*, 555 U.S. at 137); Bradley, *Red* Herring, *supra* note 18 ("[*Herring*'s holding] won't apply to the vast majority of cases, despite the apparent attempt of the majority opinion to establish a new approach to the exclusionary role [sic] that would apply to *all* cases. In most cases,

Interestingly, Tom Goldstein, a Supreme Court litigator who represented Herring, discounted this view of *Herring*'s scope. Goldstein conceded that the attenuation element temporarily contained the reach of *Herring*'s holding, but he observed that "the logic of [*Herring*] spans far more broadly, and the next logical step—which I predict is 2 years away—is abandoning the 'attenuation' reference altogether."[116] Goldstein's prediction was dead-on. When describing the type of police conduct that justifies suppression, *Davis*, decided two years after *Herring*, never mentions "attenuation."[117]

C. *What the Court's Good-Faith Exception in* Herring *and* Davis *Means for the Future of the Exclusionary Rule*

Two years ago, one of us predicted that the Roberts Court would eventually repeal the exclusionary rule.[118] We have no doubt that the Chief Justice and Justices Scalia, Thomas, and Alito are ready to abolish the exclusionary rule. But even if we are wrong about that, the logic and results in *Herring*, and now *Davis*, move the Court nine-tenths of the way toward outright abolishment. Even before the recent holding in *Davis*, *Herring*'s "big blast" statements significantly undermined and confined application of the exclusionary rule to a small number of cases. Put simply, the Chief Justice's opinion in *Herring* laid the foundation for a general good-faith exception for routine search and seizure cases.

After *Herring*, will the Court countenance the suppression of evidence obtained after an officer negligently, but in good faith, decides she has probable cause to search a car or make an arrest,

---

the police error will not be 'attenuated' from the search, but will be committed by the same officers who did the searching.").

[116] Tom Goldstein, *The Surpassing Significance of* Herring, SCOTUSBLOG (Jan. 14, 2009, 11:32 AM), http://www.scotusblog.com/2009/01/the-surpassing-significance-of-herring/.

[117] *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.3 at 28 n.181.30 (4th ed. Supp. 2011-2012) ("The *Davis* majority's 'restatement' of the *Herring* rule omits its most significant limitation, namely, that 'negligent' conduct by police supports a good-faith claim only if the negligence was 'attenuated.'").

[118] Tracey Maclin, Joseph Lipsitt Faculty Research Scholar, Bos. Univ. Sch. of L., The Fourth Amendment and the Exclusionary Rule, Address to the Hoffinger Criminal Justice Colloquium, New York University School of Law (Feb. 24, 2009).

or sufficient suspicion to conduct a *Terry* frisk? If the officer's judgment is wrong, but not culpable, and there is no proof that she has engaged in recurring violations of this kind, the logic of *Herring* dictates that exclusion is not justified. Why *would* the exclusionary rule apply in such circumstances? "[A]n officer who conducts a search that he believes complies with the Constitution but which, it ultimately turns out, falls just outside the Fourth Amendment's bounds is no more culpable than an officer who follows erroneous 'binding precedent,'"[119] or one who relies upon an arrest warrant that had been recalled five months earlier.

Or consider what Professor Richard McAdams had to say about the logic of *Herring* even when viewed as a case that merely decides the issue left open in *Arizona v. Evans*. Shortly after the oral argument in *Herring*, McAdams noted that if the Court was unwilling to distinguish between the errors of judicial employees and police employees who operate databases, the Court was unlikely to "draw a line between a sworn field officer and a police clerk."[120] As McAdams saw it, if an officer can rely in good faith on the error of a police clerk, as *Herring* now permits, she can likely rely in good faith on the error of a fellow detective. If a court will not exclude when Detective A relies on a negligent error by Detective B, then why exclude when Detective A relies on *her own* negligent, but isolated, error?[121]

If under *Herring*, only culpable or deliberate violations of the Fourth Amendment merit suppression, then a great number—perhaps the overwhelming majority—of unreasonable searches and seizures will be immunized from the exclusionary rule. After all, most search and seizure violations addressed by courts in suppression hearings across the nation involve good-faith or negligent—*not* deliberately culpable—mistakes by police officers. Before and after *Herring*, Fourth Amendment scholars made this point. The Justices know this as well.[122] Justice Breyer, however, seemed surprised, if not alarmed, by the prospect of the *Herring–Davis* logic applying to routine violations of the Fourth Amendment. He noted:

---

[119] Davis v. United States, 131 S. Ct. 2419, 2439 (2011) (Breyer, J., dissenting).

[120] Richard McAdams, *Wither the Exclusionary Rule?*, U. CHI. L. SCH. FAC. BLOG (Oct. 29, 2008), http://uchicagolaw.typepad.com/faculty/2008/10/wither-the-excl.html.

[121] *Id.*

[122] *See, e.g.*, *Davis*, 131 S. Ct. at 2439 (Breyer, J., dissenting) (explaining that most suppression motions challenge conduct where, "police, uncertain of how the Fourth Amendment applied to the particular factual circumstances they faced, will have acted in objective good faith. Yet, in a significant percentage of these instances, courts will

> [*I*]*f* the Court means what it now says, *if* it would place determinative weight upon the culpability of an individual officer's conduct, and *if* it would apply the exclusionary rule only where a Fourth Amendment violation was "deliberate, reckless, or grossly negligent," then the "good faith" exception *will* swallow the exclusionary rule.[123]

Surely Breyer knows his colleagues better than that. Of course, the Court meant what it said in *Herring* and *Davis*. That was the point of *Herring*—to confine application of the exclusionary rule to the type of purposefully, bad-faith police misconduct seen in *Mapp v. Ohio*.[124] The *Herring* majority knows that egregious Fourth Amendment violations are rarely seen in suppression hearings. Does Justice Breyer really believe that his colleagues have not made up their minds to extend the *Herring–Davis* logic to routine violations of the Fourth Amendment? Why the repeated use of the term "if" by Breyer? That is exactly what the majority intends to do. And as Breyer recognizes, some lower courts are already heading in that direction after reading *Herring*.[125]

---

find that the police were wrong."); Stewart, *supra* note 5, at 1388-89 (observing civil damages lawsuits and criminal prosecutions "punish and perhaps deter the grossest of violations, as well as governmental policies that legitimate these violations. They compensate some of the victims of the most egregious violations. But they do little, if anything, to reduce the likelihood of the vast majority of fourth amendment violations—the frequent infringements motivated by commendable zeal, not condemnable malice.").

[123] *Davis*, 131 S. Ct. at 2439 (Breyer, J., dissenting) (emphasis added).

[124] 367 U.S. 643 (1961).

[125] *See, e.g.*, United States v. Master, 614 F.3d 236, 243 (6th Cir. 2010) (noting that "the *Herring* Court's emphasis" weighed in favor of not suppressing illegally seized evidence "unless the officers engage in 'deliberate, reckless, or grossly negligent conduct'") (quoting Herring v. United States, 555 U.S. 135, 144 (2009)); United States v. Julius, 610 F.3d 60, 66-67 (2d Cir. 2010) (remanding to the district court for a determination of "whether the degree of police culpability in this case rose beyond mere administrative negligence such that application of the rule is necessary" to deter Fourth Amendment violations under the "cost/benefit analysis required by *Herring*."); United States v. Tracey, 597 F.3d 140, 151, 154 (3d Cir. 2010) (noting that "the Supreme Court has instructed that the exclusionary rule should only be applied when 'police conduct [is] . . . sufficiently deliberate that exclusion can meaningfully deter it,

D. Justice White's Roadmap for the Roberts Court's Good-Faith Exception

Perhaps one reason why judges and scholars have been reluctant to believe that the *Herring* majority really does intend to limit suppression to bad-faith or egregious search and seizure violations is the fact that the Court has never adopted this position. Although there is no precedent for this objective, Justice White provided a blueprint for reaching this goal.

In the 1970s, Justice White began urging his colleagues to adopt a good-faith exception to the exclusionary rule. White's proposal was always framed in expansive terms, even in cases where a narrower exception was available. For example, in *Stone v. Powell*,[126] Nevada police relied upon a vagrancy statute to arrest Lloyd Powell. In a companion case, Nebraska law enforcement officers obtained incriminating evidence against David Rice pursuant to a search warrant.[127] The statute and warrant were later declared unconstitutional, and the lower courts suppressed evidence obtained incident to the arrest of Powell and search of Rice's home. A majority of the Court ultimately ruled in *Stone v. Powell* that where a state has provided a defendant a full and fair opportunity to raise a Fourth Amendment claim, the Constitution does not require a state prisoner be granted federal habeas corpus relief because illegally acquired evidence was admitted at his trial.[128] In his dissent in *Stone v. Powell*, Justice White opposed restricting the remedies of habeas petitioners.[129] But White also thought that the Court should substantially limit the scope of the suppression doctrine and adopt a good-faith exception. White eschewed a modification

---

and sufficiently culpable that such deterrence is worth the price paid'" and holding that the exclusionary rule does not apply because the officer's actions did "not amount to 'deliberate, reckless, or grossly negligent conduct'" or indicate "'recurring or systemic negligence'") (citing *Herring*, 555 U.S. at 144); People v. McDonough, 917 N.E.2d 590, 594 (Ill. App. Ct. 2009) (claiming that "absent police misconduct, the exclusionary rule does not apply . . . [I]f the justification for the exclusionary rule is solely to deter police misconduct (as the Supreme Court reaffirmed in *Herring*), then the necessary condition precedent for the exclusionary rule's application is police misconduct.").

[126] 428 U.S. 465 (1976).

[127] *Id.*

[128] *Id.* at 481-82 (footnote omitted).

[129] *Id.* at 536 (White, J., dissenting).

of the exclusionary rule that would permit the admission of evidence where police either rely on a statute or warrant that is later declared invalid. Instead, White proposed a modification of the exclusionary rule that would apply in every case:

> [S]o as to prevent its application in those many circumstances where the evidence at issue was seized by an officer acting in the good-faith belief that his conduct comported with existing law and having reasonable grounds for this belief. . . . When law enforcement personnel have acted mistakenly, but in good-faith and on reasonable grounds, and yet the evidence they have seized is later excluded, the exclusion can have no deterrent effect.[130]

In the early 1980s, White continued to push for an expansive, general good-faith exception. Around the time that John Roberts finished his clerkship with Justice Rehnquist and started a four-year stint in the office of President Reagan's White House counsel, White convinced his colleagues to order reargument in *Illinois v. Gates* so that the Court could consider a good-faith exception to the exclusionary rule.[131]

White's reargument order was broadly framed. The order did not ask the parties to address whether the exclusionary rule should be modified to allow the admission of evidence obtained by police acting in reasonable reliance on a search warrant that was later declared invalid, which tracked the facts in *Gates*. White was seeking a restriction of the exclusionary rule that went beyond the facts in *Gates*. White's order asked the parties to address whether the rule should be modified when evidence was obtained "in the reasonable belief that the search and seizure at issue was consistent with the Fourth Amendment."[132] Framed this way, a good-faith exception would be available in every case of a Fourth Amendment violation and would not be confined to the narrow category of cases where police rely on a warrant that is subsequently ruled illegal.

---

[130] *Id.* at 538-40.

[131] William J. Brennan, Jr., Case Histories xxix-xxxi (Oct. Term, 1982) (on file with the Library of Congress, Manuscript Division, The William J. Brennan Papers, Box 11:7, Folder 11).

[132] Illinois v. Gates, 459 U.S. 1028, 1028 (1982).

When the parties in *Gates* submitted new briefs on the good-faith issue that the Court had asked them to address, the amicus brief filed by President Reagan's Solicitor General urged the Court to modify the exclusionary rule along the exact lines proposed by White in his *Stone v. Powell* dissent. Although the *Gates* majority ultimately decided not to reach the good-faith issue, Justice White's concurrence provided a framework for a broad good-faith exception that went beyond the facts in *Gates*. White began his *Gates* concurrence by reaffirming the position he took in *Stone v. Powell*: "[T]he exclusionary rule is an inappropriate remedy where law enforcement officials act in the reasonable belief that a search and seizure was consistent with the Fourth Amendment."[133] Acknowledging that suppression deters some police misconduct, White asserted, "it is apparent as a matter of logic that there is little if any deterrence when the rule is invoked to suppress evidence obtained by a police officer acting in the reasonable belief that his conduct did not violate the Fourth Amendment."[134]

White did not pull any punches on the scope of his good-faith exception: "There are several types of Fourth Amendment violations that may be said to fall under the rubric of 'good faith.'"[135] He recognized that a good-faith exception would be available in cases of warrantless arrests—occasions where judges disagree on the issue of probable cause, "no matter how reasonable the grounds for arrest appeared to the officer and though reasonable men could easily differ on the question."[136] But White also signaled, in a footnote discussing the concept of judicial integrity, that his good-faith exception was available where police have "reasonably erred in assessing the facts, mistakenly conducted a search authorized under a presumably valid statute, or relied in good faith upon a warrant not supported by probable cause."[137] In such cases, "the question of exclusion must be viewed through a different lens," and the "integrity of the courts is not implicated."[138] White did note, however, that exclusion would remain available for "searches and seizures perpetrated in intentional and flagrant disregard of Fourth Amendment principles."[139]

---

[133] Illinois v. Gates, 462 U.S. 213, 246 (1983) (White, J., concurring).

[134] *Id.* at 260.

[135] *Id.* at 262.

[136] *Id.* (quoting Stone v. Powell, 428 U.S. 465, 539-40 (1976) (White, J., dissenting)).

[137] *Id.* at 259 n.14.

[138] *Id.*

Although no other Justice joined White's concurrence in *Gates*, a year later White would write for a majority in *United States v. Leon*, which was the first case to adopt a good-faith exception to the exclusionary rule.[140] *Leon* held that the rule does not forbid the use in the prosecution's case-in-chief of evidence obtained by police acting in reasonable reliance on a search warrant issued by a judge but later determined to be unsupported by probable cause.[141] White also authored the companion case to *Leon*, *Massachusetts v. Sheppard*, which concluded that the exclusionary rule should be modified to permit the admission of evidence seized in reasonable reliance on a search warrant supported by probable cause but later held invalid due to the failure to specify the items to be seized.[142] Although the holdings in *Leon* and *Sheppard* were limited to cases where police obtained warrants, White sprinkled dicta throughout his opinions suggesting a good-faith exception would embrace various types of reasonable police mistakes.[143] This language was consistent with the expansive good-faith exception White had proposed in his separate opinion in *Gates* and in his dissent in *Stone v. Powell.*

Justice White's many opinions outlining the parameters of the good-faith exception provide the roadmap for the Roberts Court's goal of limiting the exclusionary rule to bad faith or egregious Fourth Amendment violations. Concededly, *Herring* and *Davis* can be read narrowly, but when it comes to the exclusionary rule, we believe that the Roberts Court does not have a narrow agenda. To ensure that the rest of the lower courts receive the message that suppression is justified only upon a showing of culpable police conduct, the Court will probably have to take a case involving a routine search and seizure violation, for example, a car search or *Terry* frisk case. If we are right about the intentions of the Roberts Court, the Court will rule that the exclusionary rule does not apply unless there is proof of culpable police conduct. If this occurs, the exclusionary rule will no longer matter. As Justice Breyer described it in his *Davis* dissent, if suppression of illegally acquired evidence is warranted only when the police are deliberately or recklessly culpable, "then the good-faith exception will swallow the exclusionary rule."[144]

---

[139] *Id.*

[140] United States v. Leon, 468 U.S. 897 (1984).

[141] *Id.* at 926.

[142] Massachusetts v. Sheppard, 468 U.S. 981, 989-91 (1984).

[143] *See, e.g.*, *Leon*, 468 U.S. at 919 (asserting that the exclusionary rule "cannot be expected, and should not be applied, to deter objectively reasonable law enforcement activity"); *id.* at 908 (noting "when law enforcement officers have acted in objective good faith or their transgressions have been minor," the benefit afforded the defendant "offends basic concepts of the criminal justice system") (citing Stone v. Powell, 428 U.S. 465, 490 (1976)); *see also* I.N.S. v. Lopez-Mendoza, 468 U.S. 1032, 1056 (1984) (White, J., dissenting) (relying on *Leon* for the assertion that if immigration officers "neither knew nor should have known that they were acting contrary to the dictates of the Fourth Amendment, evidence will not be suppressed even if it is held that their conduct was illegal").

III. BEYOND GOOD-FAITH: APPLYING *HUDSON V. MICHIGAN*'S LOGIC TO BAR SUPPRESSION AS A CATEGORICAL MATTER

Detroit, Michigan police possessed a lawful warrant to search for drugs and guns in Booker Hudson's home. After announcing their presence, police waited only three to five seconds before entering. Inside they found Hudson, drugs, and a gun.[145] After Hudson was convicted of narcotics and gun possession, Michigan prosecutors conceded the manner of entry violated the Fourth Amendment's knock-and-announce rule.[146] Thus, the only issue confronting the Justices in *Hudson v. Michigan* was whether suppression is appropriate when police infringe the knock-and-announce rule.[147]

A. Justice Scalia's Three Rationales in Hudson

Justice Scalia's opinion for the Court in *Hudson* held that suppression is never a remedy for knock-and-announce violations. Scalia's ruling rested on three distinct and independent bases. First, he explained that the unlawful entry "was *not* a but-for cause of obtaining the evidence."[148] The failure to comply with the announcement rule had no causal nexus to obtaining the evidence because whether the police would have complied with the Constitution or not, they would have executed the warrant and discovered the evidence. This conclusion was sufficient to affirm Hudson's conviction and end the case, but Scalia had more on his mind.[149]

---

[144] Davis v. United States, 131 S. Ct. 2419, 2439 (2011) (Breyer, J., dissenting).

[145] Hudson v. Michigan, 547 U.S. 586, 588 (2006).

[146] *Id.* at 590.

[147] While Justice Scalia's opinion does not frame the issue this way, surely this *was* the issue addressed and decided by the Court. *See* Tomkovicz, *the Future*, *supra* note 9, at 1822, 1823 nn.13 & 19.

[148] *Hudson*, 547 U.S. at 592.

Second, Scalia explained that even if the constitutional violation was the but-for cause of obtaining the evidence, admission of the evidence is nevertheless proper when the connection between the police illegality and the discovery of the evidence is "too attenuated to justify exclusion."[150] Here, Scalia invoked the attenuation exception to the exclusionary rule. He accurately noted that in prior cases, suppression was denied where the nexus between the Fourth Amendment violation and the seizure of evidence was "remote."[151] Although Scalia did not acknowledge it, this traditional attenuation exception was unavailable in *Hudson* since the discovery of the evidence immediately followed on the heels of the illegal entry, and there were no intervening circumstances that severed the connection between the violation and discovery.[152]

Undeterred by prior precedent, Justice Scalia created a new form of attenuation. He explained, "Attenuation also occurs when, even given a direct causal connection, the interest protected by the constitutional guarantee that has been violated would not be served by suppression of the evidence obtained."[153] Scalia then noted that the interests protected by the announcement rule included protecting human life and limb, preventing the destruction of property, and protecting aspects of privacy and dignity that can be disturbed by a sudden entry. Scalia then distinguished these interests from the interest protected by the warrant requirement.[154] When police violate the warrant requirement, Scalia explained, the government infringes a person's right to "shield 'their persons, houses, papers, and effects from the government's scrutiny."[155] Exclusion of evidence obtained in violation of the warrant requirement "vindicates that entitlement."[156] The knock-and-announce rule, however, does not protect a person's interest in precluding police from seizing evidence described in a valid warrant. Thus, Scalia concluded: "Since the interests that *were* violated in [*Hudson*] have nothing to do with the seizure of the evidence, the exclusionary rule is inapplicable."[157]

---

[149] *See also* Tomkovicz, *the Future*, *supra* note 9, at 1825 ("Justice Scalia could have ended his opinion at this point. His conclusion about the absence of a causal connection between the knock-and-announce violation and the discoveries in the home foreclosed application of the *Mapp* rule to this case. Justice Scalia continued, however, turning to additional, broader grounds for declaring the [exclusionary] rule inapplicable to Hudson's gun and drugs."); *id.* at 1825 n.31 ("The fact that [Scalia] did not pen a short, simple opinion that rested solely on the absence of causation is just one of many indications that the *Hudson* majority was bent upon accomplishing more than simply eliminating the exclusionary remedy for knock-and-announce violations.").

[150] *Hudson*, 547 U.S. at 592.

[151] *Id.* at 593.

[152] *See also* Tomkovicz, *the Future*, *supra* note 9, at 1863-64 (The evidence found in Hudson's home was "primary, immediately acquired products, not derivative evidence with a weakened connection to the unconstitutionally hasty entry.").

[153] *Hudson*, 547 U.S. at 593.

The third basis for *Hudson*'s holding was that "the exclusionary rule has never been applied except where its deterrence benefits outweigh its substantial social costs."[158] The origins of this amorphous balancing test dates back to *Alderman v. United States*,[159] and the test has been a central element of the Court's exclusionary rule cases ever since.

The objective of this section is not to assess the merits of Scalia's legal reasoning in *Hudson*. Other scholars, including Professors Al Alschuler, Sharon Davies, Eric A. Johnson, Wayne LaFave, and James Tomkovicz, have already superbly performed that task, and we recommend reading their analyses.[160] Rather, our goal is to consider what *Hudson*'s attenuation analysis means for the future of suppression law. We think *Hudson*'s novel attenuation rule was designed to apply to search and seizure violations beyond the announcement rule. In addition, we believe that Scalia wrote *Hudson* to lay the foundation for abolishing suppression generally. In other words, Scalia's analysis in *Hudson* is *not* a "good-for-this-train-only" ticket. Rather, it is intended specifically for use in future cases to bar suppression as a categorical matter, and *Hudson* itself, as a general matter, was structured to provide a blueprint for repealing the exclusionary rule when five Justices are ready to do so.

---

[154] *Id.* at 593-94.

[155] *Id.* at 593 (quoting U.S. CONST. amend. IV).

[156] *Id.*

[157] *Id.* at 594.

[158] *Id.* (quoting Pa. Bd. of Prob. & Parole v. Scott, 524 U.S. 357, 363 (1998)) (internal quotation marks omitted).

[159] 394 U.S. 165 (1969).

[160] *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.6(h) at 43-49 (4th ed. Supp. 2011-2012); 6 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 11.4 at 44-48 (4th ed. Supp. 2011-2012); *id.* § 11.4 at 52-60; Eric A. Johnson, *Causal Relevance in the Law of Search and Seizure*, 88 B.U. L. REV. 113 (2008); Alschuler, *Exclusionary Rule*, *supra* note 27; Davies & Scanlon, *supra* note 34; Tomkovicz, *the Future*, *supra* note 9. For a thorough survey of the lower courts' use of *Hudson's* logic, see Christopher D. Totten, *The Exclusionary Rule After* Hudson v. Michigan*: Mourning the Death of the Knock and Announce Rule*, 46 No. 5 CRIM. L. BULL. art. 1 (Fall 2010).

B. Two Different Forms of Attenuation: Traditional and Hudson v. Michigan *Attenuation*

From its inception, attenuation analysis was designed to curtail application of the exclusionary rule. The concept of attenuation originated in Justice Frankfurter's opinion in *Nardone v. United States*[161] as a way for the government to bypass the exclusionary rule and admit illegally acquired evidence. According to Frankfurter, it was "a matter of good sense" that the connection between an illegal search and the evidence proffered by the government at trial "may have become so attenuated as to dissipate the taint."[162] Although *Nardone* was not a Fourth Amendment case, and Frankfurter's thoughts on attenuation were obiter dictum, twenty years later *Wong Sun v. United States* adopted Frankfurter's analysis to determine when evidence obtained from a Fourth Amendment violation was subject to exclusion.[163] Around the same time, Professor Anthony Amsterdam, a former Frankfurter clerk, characterized the attenuation doctrine as "foggy" and "inarticulately and unsystematically designed."[164] Yet, he recognized that the purpose of attenuation analysis was "to mark the point of diminishing returns of the deterrence principle" of the exclusionary rule.[165]

---

[161] 308 U.S. 338 (1939).

[162] *Id.* at 341.

[163] 371 U.S. 471 (1963).

[164] Anthony G. Amsterdam, *Search, Seizure, and Section 2255: A Comment*, 112 U. PA. L. REV. 378, 389-90 (1964).

[165] *Id.* at 390.

As an exception to the exclusionary rule, traditional attenuation only applies to derivative evidence because the nexus between an illegal search and direct or primary evidence (e.g., evidence seized from the pocket of a person illegally arrested) "is both proximate and strong, not 'remote' or 'attenuated.'"[166] During the 1960s and 1970s, attenuation analysis "probed the strength of the connection between the police illegality and the evidence the prosecutor wished to introduce by examining the circumstances under which the evidence came into the hands of the police."[167] But the Court's rulings also rejected per se or absolute formulas proposed by the government to circumvent exclusion.[168] As Justice Powell described it, "the question of attenuation inevitably is largely a matter of degree."[169] In sum, although designed to take some of the bite out of the exclusionary rule, traditional attenuation analysis, at least as practiced by the Court prior to *Hudson*, paralleled the deterrence purposes of the exclusionary rule.

It is important to understand that the type of attenuation adopted in *Hudson* is not only novel and expansive,[170] but it also drastically differs from a traditional attenuation analysis. As Professor Tomkovicz explains in his recent book on constitutional exclusion:

---

[166] Tomkovicz, *the Future*, *supra* note 9, at 1863.

[167] Davies & Scanlon, *supra* note 34, at 1060.

[168] For example, in *Brown v. Illinois*, 422 U.S. 590 (1975), the Illinois attorney general urged the Court to adopt a per se rule that *Miranda* warnings were sufficient to dissipate the taint of an illegal arrest and thus allow the admission of the defendant's statement given while in police custody. *Id.* The Court rejected that rule and instead employed a multi-prong test to determine whether a confession was obtained by exploitation of an illegal arrest. *Id.* at 603-04. Similarly, in *United States v. Ceccolini*, 435 U.S. 268 (1978), the government argued that live witness testimony was never tainted fruit no matter how direct the nexus between an illegal search and the testimony. *Id.* Again, the Court rejected the proposed per se rule in favor of a multi-factor balancing test. *Id.* at 274, 276-80. *But cf.* New York v. Harris, 495 U.S. 14, 21 (1990) (deciding in what amounted to a per se rule, that where police have probable cause to arrest a suspect, the exclusionary rule does not bar the admission of a voluntary confession given by the suspect outside of his home, even though the confession is taken after an arrest in the home that violates the rule of *Payton v. New York*, 445 U.S. 573 (1980)). The connection between the results in *Hudson* and *Harris* have been analyzed by Professor Eric Johnson. *See* Johnson, *supra* note 160.

[169] *Brown*, 422 U.S. at 609 (Powell, J., concurring in part).

[170] Tomkovicz, *the Future*, *supra* note 9, at 1863; Davies & Scanlon, *supra* note 34, at 1061.

> "Attenuation" seems like a misnomer for this alternative version of the exception. The connection between the violation and the evidence at issue can be very close and very strong. Indeed, this offshoot of the attenuation doctrine encompasses even *primary* evidence acquired as an immediate result of a Fourth Amendment violation and is unconcerned with the culpability of the officers or the egregiousness of their transgression. Considering its very different character, it is at least odd to pair it with the traditional form of the attenuation.[171]

C. Extending Hudson*'s Attenuation Logic Beyond the "Knock-and-Announce" Context*

It is also imperative to appreciate how easily *Hudson*'s attenuation analysis can be employed to admit evidence in cases of other search and seizure violations. Under *Hudson*, the exclusionary rule applies only when excluding evidence serves the constitutional interest promoted by the Fourth Amendment rule that the police have failed to follow. The Court could extend *Hudson's* logic to bar suppression in a number of contexts.

1. *Hudson* and the "No Press" Rule

The logic of *Hudson*'s attenuation rule bars exclusion when the *manner* of a police entry into a home violates the Constitution. Thus, exclusion is never appropriate when the police allow journalists or other third parties to accompany them when they enter a home to make an arrest or conduct a search. A decade ago, *Wilson v. Layne* found this practice unconstitutional because the Fourth Amendment requires that police actions in execution of a warrant be "related to the objectives of the authorized intrusion," and, as a general matter, the presence of reporters in a home does not aid the police in executing a warrant.[172] While *Wilson* did mention the "privacy" afforded the home, the Court was also careful to observe that the Fourth Amendment violation "is the presence of the media and not the presence of the police in the home," and thus it was reserving the question "whether the exclusionary rule would apply to any evidence discovered or developed by the media representatives."[173] Despite the ruling in *Wilson*, television news programs continue to show videos of police raiding private homes and businesses, indicating that *Wilson* is still being violated in some locales. But after *Hudson*, there is no reason to think the Court will countenance exclusion for this offense. The Court could easily use *Hudson*'s attenuation logic to conclude that suppression does not vindicate the interests for excluding the media and hold that the exclusionary rule is inapplicable.

---

[171] TOMKOVICZ, *supra* note 1, at 51.

[172] Wilson v. Layne, 526 U.S. 603, 611 (1999).

2. *Hudson* and the "Right-to-See-a-Warrant" Rule

Similarly, the Court has not definitively decided whether a homeowner has a right, circumstances permitting, to inspect a warrant before police enter a home to effectuate a search or an arrest. Language from some of the Court's rulings implicitly recognizes a homeowner's right to inspect a warrant before police entry. Over forty years ago, *Camara v. Municipal Court* acknowledged the dilemma facing a homeowner when confronted with a municipal inspector's demand to perform a warrantless search of his home: The homeowner "has no way of knowing whether enforcement of the municipal code involved requires inspection of his premises, no way of knowing the lawful limits of the inspector's power to search, and no way of knowing whether the inspector himself is acting under proper authorization."[174]

Similarly, *Wilson v. Arkansas* ruled that the common law knock-and-announce requirement was constitutionally based.[175] One of the interests served by the common law announcement rule was to allow a homeowner the opportunity to demand identification from officers seeking entry and to allow the resident to explain to the officers that the person or premises were mistakenly described in the warrant.[176] Of course, these purposes could not be served if the homeowner had no right to see the warrant before police entry.

---

[173] *Id.* at 614 n.2.

[174] Camara v. Mun. Ct. of S.F., 387 U.S. 523, 532 (1967).

[175] Wilson v. Arkansas, 514 U.S. 927 (1995).

[176] *See* Charles P. Garcia, Note, *The Knock and Announce Rule: A New Approach to the Destruction-of-Evidence Exception*, 93 COLUM. L. REV. 685, 687-88 (1993).

Finally, when *Groh v. Ramirez* explained why the presence of a search warrant serves a high function (that could not necessarily be vindicated by some other document not made available to the homeowner), the Court suggested that a homeowner could see the warrant "for her inspection" before police entry.[177] These statements provide the basis for concluding that a homeowner has a constitutional right to see a warrant prior to entry. That right would protect, *inter alia*, an occupant's interest in assuring that the entry was lawful, the occupant is informed of the scope of the power of the police to search or seize, and that the police are acting under proper authority.

To be sure, more recently in *United States v. Grubbs*, Justice Scalia's majority opinion observed in dictum that the Fourth Amendment imposed no requirement to present a homeowner with a warrant.[178] Justice Souter's concurrence, however, pointed out that the Court had previously reserved that question in *Groh v. Ramirez*, and that it remained unsettled after *Grubbs*.[179] Souter observed that displaying a warrant to a homeowner "assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search."[180]

Assuming the Court will find that the Fourth Amendment grants a homeowner a right to see a warrant before a police entry, *Hudson*'s attenuation logic ensures that exclusion will never be an appropriate remedy where police violate this right and discover evidence in a subsequent search. As in *Hudson*, the Fourth Amendment interests protected by a "right-to-see-a-warrant" are different from and "do not include the shielding of potential evidence from the government's eyes."[181] In fact, in *United States v. Hector,* the Ninth Circuit used *Hudson's* attenuation reasoning to conclude that the exclusionary rule does not apply when the police fail to present the defendant with a search warrant.[182]

---

[177] Groh v. Ramirez, 540 U.S. 551, 557 (2004).

[178] United States v. Grubbs, 547 U.S. 90, 98 (2006).

[179] *Id.* at 101 (Souter, J., concurring in part and concurring in the judgment).

[180] *Id.* (quoting United States v. Chadwick, 433 U.S. 1, 9 (1977)).

[181] Hudson v. Michigan, 547 U.S. 586, 593 (2006).

[182] United States v. Hector, 474 F.3d 1150, 1155 (9th Cir. 2007), *cert. denied*, 552 U.S. 1104 (2008).

After obtaining a lawful warrant, Los Angeles police pried open Albert Hector's door to search his apartment for drugs and related paraphernalia. During the search, the officers showed Hector a "Search Warrant Notice of Service," which was not the actual search warrant and did not contain the address of the location to be searched or list the items to be seized. The police did not show Hector the warrant at any time during the search. At Hector's apartment, the police found drugs, money, and a loaded handgun.[183] The jury found Hector guilty of drug and weapons offenses based on evidence found in his apartment. After the jury verdict, Hector moved to suppress the evidence. The district court granted the motion and "held that the officers' failure to serve Hector the search warrant violated the Fourth Amendment and required suppression of the evidence."[184]

The Ninth Circuit reversed. Relying on *Hudson*'s attenuation analysis, the court ruled that regardless of whether the failure to serve a copy of the warrant was a violation of the Fourth Amendment, exclusion was inappropriate.[185] The Ninth Circuit, embracing *Hudson*'s logic, found that "[t]he causal connection between the failure to serve the warrant and the evidence seized is highly attenuated, indeed nonexistent, in this case."[186] The court noted that the only legitimate interest served by presenting the warrant after *Grubbs* "is to head off breaches of peace by dispelling any suspicion that the search is illegitimate."[187] The court explained that this interest, like the interests promoted by the announcement rule, does not involve the "seizure of evidence described in the search warrant nor would it be vindicated by suppression of the evidence seized."[188] Accordingly, the Ninth Circuit concluded that under *Hudson*'s logic, suppression was unwarranted.[189]

Similarly, the district court in *United States v. Makki* relied on *Hudson*'s attenuation logic and the Ninth Circuit's analysis in *Hector* to hold that exclusion was not an appropriate remedy when the police failed to show the defendant the list of items to be seized pursuant to a search warrant.[190] The court found that "the causal connection between any failure to provide Defendant with a list of the items to be seized and the evidence actually seized is 'highly attenuated, indeed non-existent.'"[191] The court further explained that the interest promoted by presenting the list of items in the warrant—"head[ing] off breaches of the peace by dispelling any suspicion that the search is illegitimate . . . does not implicate the seizure of evidence . . . ."[192] The court concluded that suppression would not vindicate the interest that was violated.[193] "[I]n light of the rationale of the exclusionary rule and the considerations set out by the Supreme Court in *Hudson*," the district court found suppression an inappropriate remedy.[194]

---

[183] *Id.* at 1153.

[184] *Id.*

[185] *Id.* at 1155.

[186] *Id.*

[187] *Id.* (quoting United States v. Stefonek, 179 F.3d 1030, 1035 (7th Cir. 1999)).

[188] *Id.*

[189] *Id.*

Because the interests served by showing a warrant are separate from a person's interest in precluding police from seizing evidence described in that warrant, *Hudson*'s reasoning easily extends to bar suppression after the police fail to present a search warrant. Thus, as some courts have already recognized, *Hudson*'s attenuation logic will ensure that even if the Court finds that the Fourth Amendment protects a person's "right-to-see-a-warrant," the exclusionary rule will not apply to violations of this right.

3. *Hudson* and the "No Arbitrary Destruction of Property" Rule

Hudson's attenuation analysis would also seem to bar exclusion where police arbitrarily destroy property while executing a warrant. In *United States v. Ramirez*, the Court stated in dictum: "Excessive or unnecessary property destruction during a search may violate the [Fourth] Amendment, even though the entry itself is lawful and the fruits of the search not subject to suppression."[195] And *Ramirez* reserved whether, if breaking a window to enter a garage violated the Fourth Amendment, there was a "sufficient causal relationship" between the breaking and the discovery of evidence to justify suppression.[196] However, even assuming a direct connection between the breaking and the discovery of evidence, *Hudson*'s attenuation theory would bar suppression because the constitutional interest protected here—preservation of property—is unrelated to and does not "include the shielding of potential evidence from the government's eyes."[197]

---

[190] United States v. Makki, No. 06-20324, 2007 WL 1100453, at *4 (E.D. Mich. Apr. 12, 2007).

[191] *Id.* (quoting United States v. Hector, 474 F.3d 1150, 1155 (9th Cir. 2007)).

[192] *Id.*

[193] *Id.*

[194] *Id.*

[195] United States v. Ramirez, 523 U.S. 65, 66 (1998).

Professor Tomkovicz has written that "[i]t would seem" that *Hudson*'s attenuation analysis is applicable "to violations of other [constitutional] rules that prescribe the constitutional *manner* of home entries or other searches."[198] We agree with his conclusion, but without the cautious qualification. We see no principled difference in the conclusion that the announcement rule does not promote the "shield" function identified by Justice Scalia's new attenuation theory, and the conclusion that the "no press" rule, the "right-to-see-a-warrant" rule, and the "no arbitrary destruction of property" rule, also do not promote the "shield" function.

4. *Hudson* and the "Inventory Search" Rules

Professor Tomkovicz also believes that *Hudson*'s attenuation theory is potentially applicable "to any case involving evidence found as a result of an unconstitutional *seizure* of a person or property."[199] According to Tomkovicz:

> The Fourth Amendment's prohibitions of unreasonable seizures of individuals and effects are arguably designed to serve liberty and possessory interests, respectively, not to shield potential evidence from government eyes. According to the logic of *Hudson*, because suppression does not serve the interests beneath those rules, the exclusionary rule is inapplicable.[200]

---

[196] *Id.* at 72 n.3. In *Hudson*, Justice Scalia, speaking for four Justices, viewed *Ramirez*'s reservation of this issue as a clear expression of the "proposition that an impermissible manner of entry does not necessarily trigger the exclusionary rule." Hudson v. Michigan, 547 U.S. 586, 602 (2006).

[197] *Hudson*, 547 U.S. at 593.

[198] Tomkovicz, *the Future*, *supra* note 9, at 1864-65 (footnote omitted).

[199] *Id.* at 1865.

[200] *Id.*

Again, we agree with Tomkovicz's judgment. Just as rational persons could determine that exclusion does not advance the purposes behind the constitutional bar on unreasonable seizures, rational persons could also decide that exclusion does not advance the purposes the Court has identified in its inventory search cases. In several cases, the Court has upheld the government's power to conduct inventory searches of impounded cars and an arrestee's effects. The searches involved can be quite extensive, like the search in *Colorado v. Bertine*, which included the detailed inspection of a backpack located inside a vehicle after the owner of the vehicle had been arrested for driving under the influence.[201] The *Bertine* Court, relying on earlier inventory search cases, *South Dakota v. Opperman*[202] and *Illinois v. Lafayette*,[203] held that the police do not violate the Fourth Amendment when they discover evidence pursuant to departmental standardized guidelines for inventory searches. These cases explain that neither the warrant nor probable cause requirements govern inventory searches.[204] Because inventory searches are not designed to advance criminal investigations, traditional Fourth Amendment safeguards, like a magistrate's independent determination that a search is proper or individualized suspicion of wrongdoing, are inapplicable.[205] The Court has also explained that the purposes served by inventory searches include protecting a person's property while in police custody; guarding the government against frivolous lawsuits over lost, stolen, or vandalized property; and protecting police safety.[206] Thus, the Court has authorized inventory searches if law enforcement agencies provide standardized guidelines to control police discretion when conducting such searches.

---

[201] Colorado v. Bertine, 479 U.S. 367, 368-69 (1987). In the backpack, the officer came across a nylon bag containing metal canisters. *Id.* at 369. After opening the canisters, the officer found drugs, drug paraphernalia, and cash. *Id.* He also discovered cash in a *sealed* envelope located in a zippered outside pocket of the backpack. *Id.* The officer took the backpack and its contents to the police station, and Bertine was charged with possession and intent to sell the drugs. *Id.*

[202] 428 U.S. 364, 369 (1976) (holding that the police's search of a closed glove compartment pursuant to a routine inventory search of a lawfully impounded car did not violate the Fourth Amendment).

[203] 462 U.S. 640 (1983) (holding that the inventory search of an arrestee's personal effects at the police station did not violate the Fourth Amendment's warrant requirement).

[204] *See Opperman*, 428 U.S. at 367 (noting that although vehicles are "effects" within the reach of the Fourth Amendment, the inherent mobility of cars and the reduced expectation of privacy within a vehicle makes "rigorous enforcement of the warrant requirement . . . impossible"). *See generally Lafayette*, 462 U.S. 640.

[205] *Bertine*, 479 U.S. at 371.

Keeping in mind the constitutional interests served by inventory searches, we see no reason why suppression is warranted when police conduct an illegal inventory search. As in *Hudson*, the interests protected by the Court's inventory cases "are quite different—and do not include the shielding of potential evidence from the government's eyes."[207] Thus, even if an officer conducts an unreasonable inventory search by ignoring standardized procedure, the Court will find suppression inappropriate. Because the interests served by inventory searches—safeguarding an owner's property; shielding the government from lawsuits over lost, stolen, or vandalized property; and promoting police safety—"have nothing to do with the seizure of . . . evidence," the Court will likely rule, using *Hudson*'s attenuation logic, that the exclusionary rule is inapplicable.[208]

In sum, while Justice Kennedy may believe that after *Hudson* the exclusionary rule remains functioning, there is good reason to believe that *Hudson*'s attenuation theory was designed to restrict future applications of the rule. We believe that *Hudson*'s attenuation theory will not be confined to the context of police violations of the knock-and-announce rule. By insisting that the suppression doctrine only applies when exclusion will promote the underlying Fourth Amendment value the police have violated, *Hudson* brazenly contradicted the notion that exclusion was not intended to vindicate a defendant's constitutional rights.[209]

---

[206] *Id.* at 372.

[207] Hudson v. Michigan, 547 U.S. 586, 593 (2006).

[208] *Id.* at 594.

[209] Professor Alschuler cogently explains why *Hudson*'s analysis contradicts a central tenant of the Burger and Rehnquist Courts:

> For more than forty years, the Court has denigrated "rights" theories of the [exclusionary] rule and contended that exclusion never vindicates the interests of the defendant before the court. The Court has insisted that exclusion is always what the *Hudson* Court said it never can be—a windfall awarded to a defendant for the sake of protecting the rights of others. If, as the Court has said repeatedly, exclusion cannot restore the defendant's violated interests and is not designed to do so, *Hudson*'s declaration that

Moreover, Scalia's opinion takes a long stride toward eventual abolition of the exclusionary rule.

CONCLUSION

We believe that the Court is already implementing its "reassessment" of the exclusionary rule. If we are right about the intentions of the Roberts Court, the Court will take a case involving a routine search and seizure violation and rule that the exclusionary rule does not apply unless there is proof of culpable or egregious police conduct. If this occurs, the exclusionary rule will no longer matter—nor will the protections of the Fourth Amendment.

> exclusion is inappropriate *unless* it restores the defendant's violated interests is simply a formula for abolishing the rule.

Alschuler, *Exclusionary Rule*, *supra* note 27, at 1764 (footnote omitted). We believe it is incredible that Justice Scalia was unaware of the inconsistency between the conclusion that exclusion is not a personal right and his newly announced theory in *Hudson*. Scalia is simply too smart and savvy not to have noticed the conflict. This is another example of Scalia's, and the conservative majority's, willingness to find or create theories to promote their anti-exclusionary rule agenda. *See id.* at 1756 ("The Court shifts to whichever reason for exclusion gives it a reason not to exclude.").

FOURTH AMENDMENT FUTURE: REMOTE COMPUTER SEARCHES AND THE USE OF VIRTUAL FORCE

*Susan W. Brenner**

INTRODUCTION 1229
I. TROJAN HORSE WARRANTS? 1232
  A. Europe 1232
  B. United States 1237
  C. Search 1238
  D. Seizure 1244
  E. Trojan Horse Warrants 1246
  F. Exceptions 1251
II. VIRTUAL FORCE? 1253
CONCLUSION 1259

INTRODUCTION

For roughly the first 130 years of its existence, the Fourth Amendment, unlike other components of the Bill of Rights, was not a problematic constitutional provision.[1] It started to become problematic in the 1920s, as new technologies—such as automobiles and telephones—became more widely used.[2]

As the twentieth century progressed, the Fourth Amendment's applicability (or inapplicability) to the technologies that emerged and matured after 1900, but before 2000, was more

---

* NCR Distinguished Professor of Law and Technology, University of Dayton School of Law, Dayton, OH. Email: susanwbrenner@yahoo.com.

[1] The Bill of Rights became effective on December 15, 1791. *See, e.g.*, LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 42-43 (2001).

[2] *See, e.g.*, Thomas K. Clancy, Symposium, *The Effect of Technology on Fourth Amendment Analysis and Individual Rights,* 72 MISS. L.J. 1, 2-3 (2002) (noting Supreme Court cases dealing with twentieth-century technologies); *see also* Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technology,* 80 MISS. L.J. 1131, 1138-40 (2011).

or less settled.[3] Ambiguities and uncertainties remain in certain areas, but the Fourth Amendment jurisprudence of the pre-twenty-first century technologies is relatively stable.[4]

That is not true of the digital technologies that emerged in the last decades of the twentieth century and have been evolving in sophistication and complexity ever since. Unlike their essentially stable predecessors, which tended to have specific uses, these technologies infiltrate many, if not most, areas of human endeavor.[5] We use them to communicate, to create, to navigate, to heal, to manufacture, to educate, to forecast, to research, to surveil, to attack, etc.

Perhaps the feature that most distinguishes these technologies from their more mundane predecessors is that they facilitate human activity in what is—or in what we experience as—a non-physical context. Computers and other electronic devices let us "go into" cyberspace, which, of course, is not a "space" at all, but is a conduit we can use to generate effects—consequences—that are felt in the physical world.[6]

The pervasiveness and consequential nature of digital technologies make them an increasingly important aspect of our lives, which means, among other things, that they are used by the lawless as well as the law-abiding. In the 1920s, the Supreme Court was called upon to determine the Fourth Amendment's applicability to two still novel technologies—automobiles and telephones—because criminals quickly grasped how they could be exploited to facilitate the commission of unlawful acts.[7]

And law enforcement officers soon grasped how they could exploit these new technologies to facilitate their pursuit of those who committed unlawful acts.[8] Law enforcement's use of automobiles raised few, if any, Fourth Amendment issues, but its use of telephone surveillance produced the first case in which the Supreme Court was required to consider the implications of technology that transcends the limitations of physical reality.[9]

---

[3] *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 862-64 (2004) (noting that the use of "stable" technologies facilitates the articulation of stable rules derived from the Fourth Amendment).

[4] *See, e.g.*, *id.* at 860-64.

[5] *See generally* SUSAN W. BRENNER, LAW IN AN ERA OF "SMART" TECHNOLOGY (2007); *see also* Kerr, *supra* note 3, at 864-65.

[6] *See, e.g.*, Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology, and the Constitution*, 7 J. TECH. L. & POL'Y 123, 144-45 (2002).

[7] *See id.* at 150-53; *see also* SUSAN W. BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE 156 (Frankie Y. Bailery & Steven Chermak eds., 2010).

As many have noted, the Supreme Court misapprehended the implications of that technology, issuing a decision that was predicated on the spatial notion of privacy that had prevailed and sufficed, until that point in our history.[10] It was not until 1967 that the Court shifted away from that approach to one that is more conceptual but still retains a concern with spatial privacy.[11]

Courts now find themselves grappling with technologies that far surpass twentieth-century telephones in complexity and application. As one author noted, judges are attempting to determine the Fourth Amendment's applicability to "intrusive scanning machines, . . . handheld devices the police can use to measure the presence of alcohol on one's breath and guns and drugs on the person's body; facial recognition systems . . . and very sophisticated systems to search e-mail and computer files."[12] Of course, these are only a few of the technologies already in use that have the capacity to be exploited by law enforcement and that therefore give rise to difficult Fourth Amendment issues.[13]

These issues arise because, as our experience with automobiles and telephones illustrates, law enforcement is quick to grasp, and exploit, the enhanced capabilities new technologies provide. My goal in this Article is to project how law enforcement can and, I suspect, will, utilize two as yet unexploited aspects of digital technology: (1) the use of Trojan Horse software to conduct surreptitious, remote searches of computers[14] and (2) the use of computer software and/or signals as "virtual force" to shut down criminal websites or otherwise impede unlawful online activity. The first section below examines remote computer searches; the next section examines virtual force.

---

[8] *See, e.g.*, BRENNER, CYBERCRIME, *supra* note 7, at 158.

[9] *See, e.g.*, Brenner, *Privacy Privilege*, *supra* note 6, at 144-45; *see also* Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 20-25 (2005).

[10] *See, e.g.*, Brenner, *Ubiquitous Technology*, *supra* note 9, at 4-25.

[11] *See id.* at 25-28.

[12] Clancy, *supra* note 2, at 3.

[13] *Id.* at 4.

[14] A Trojan horse program "is a malicious code concealed within an apparently harmless [computer] program that hides its true function." U.S. DEP'T OF JUSTICE, NAT'L INST. OF JUSTICE, INVESTIGATIONS INVOLVING THE INTERNET AND COMPUTER

I. TROJAN HORSE WARRANTS?

In examining the likelihood that U.S. law enforcement will eventually use Trojan Horse programs to conduct remote searches of computers, I need to address two issues. One issue essentially involves precedent—in the subsection immediately below, I review efforts to authorize the use of such searches in Europe. In the next subsection, I analyze the Fourth Amendment issues that would have to be addressed before U.S. law enforcement agencies could lawfully utilize such searches.

A. Europe

In a press release issued at the end of 2008, the European Union (EU) announced a new five-year plan to target cybercrime.[15] Among other things, the plan called for law

---

NETWORKS 55 (2007), *available at* http://www.ncjrs.gov/pdffiles1/nij/210798.pdf. Trojan Horse programs are routinely used by cybercriminals to steal information from unwary computer users or to take control of their computers. *See id.* at 1. As Timothy C. MacDonnell notes, they could also be used by law enforcement:

> In the context of the home, the government could send an email to a suspect that contains a "Trojan horse" program. Once the email was opened the program could be downloaded to the suspect's computer without his knowledge. The program would search the target computer for the hash value of known contraband files. If the program encountered a contraband file, it would alert law enforcement.

Timothy C. MacDonnell, *Orwellian Ramifications: The Contraband Exception to the Fourth Amendment*, 41 U. MEM. L. REV. 299, 346-47 (2010) (footnotes omitted); *see id.* at 347 n.335 (noting that Trojan Horse programs let the operator of the software retrieve user names and passwords stored on the target computer and "find, view, copy and delete files," among other things).

[15] *See* Press Release, Europa, Fight against Cyber Crime: Cyber Patrols and Internet Investigation Teams to Reinforce the EU Strategy (Nov. 27, 2008), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827 ("Cyber crime is a growing threat to our societies today. EU member states suffer daily thousands of attacks against their information systems. . . . The European Commission has cooperated closely with the French Presidency and the Member States in the elaboration of a series of practical measures to fight cyber crime. The new strategy

enforcement officers in EU member states to conduct "remote searches" of computers.[16]

A few months earlier:

> [T]he EU Council Presidency circulated a Note on a: "*Comprehensive plan to combat cyber crime*" to COREPER - the Council committee of Brussels-based high-level representatives of each Member State.[17]
>
> Under the sub-heading "The emergence of new issues" it said that there were some: "projects already in existence" which require "common approaches" including:
>
> "the area of remote computer searches, which are a delicate issue because of their cross-border nature." (emphasis added)
>
> Reading between the lines the phrase: "projects already in existence" implies that state agencies in some Member States are already conducting cross-border remote computer searches both in their home countries and across borders in other states.[18]

---

recommends reinforcing partnership between the police and the private sector by better knowledge-sharing on investigation methods and trends in cyber crime. It also encourages both parties to respond quickly to information requests, resort to remote searches, cyber patrols for online tracking of criminals and joint investigations across borders."); *see also EU to Search out Cyber Criminals*, BBC NEWS (Dec. 1, 2008, 10:57 GMT), http://news.bbc.co.uk/2/hi/technology/7758127.stm.

[16] *See* BBC NEWS, *supra* note 15.

[17] Tony Bunyan, *EU Agrees Rules for Remote Computer Access by Police Forces—But Fails, as Usual, to Mention—the Security and Intelligence Agencies*, 19 STATEWATCH J., Aug. 2009, at 1, *available at* http://www.statewatch.org/analyses/no-83-remote-computer-access.pdf; *see also* Lesley Dingle & Bradley Miller, *A Summary of Recent Constitutional Reform in the United Kingdom*, 33 INT'L J. LEGAL INFO. 71, 94 (2005) ("'The Council [of the European Union] is the main decision-making body of the European Union . . . [its] acts . . . can take the form of regulations, directives, decisions, . . . recommendations or opinions. The Council can also adopt conclusions . . . . When the Council acts as a legislator, in principle it is the European Commission that makes proposals. These are examined within the Council, which can modify them before adopting them.' The Council is obliged to 'consult' [the European] Parliament on its acts, . . . but should disagreement arise, the Council can dispense with Parliament's opinion." (footnotes omitted)).

[18] Bunyan, *supra* note 17, at 2.

This note became the basis of a "proposal for formal Council 'Conclusions,'" which eventually called for "measures to facilitate remote computer searches, allowing investigators rapid access to data."[19] The final, adopted version called for "facilitating remote searches if provided for under national law, enabling investigation teams to have rapid access to information, with the agreement of the host country."[20]

Neither the initial press release nor the subsequent news stories explained precisely what these "remote searches" would involve. Some speculated that they might involve using remotely installed keystroke loggers, an updated version of the Federal Bureau of Investigation's "Magic Lantern" program.[21] According to one source, the FBI created Magic Lantern

> primarily to overcome the problems raised by suspects who were savvy enough to encrypt their data. It operates in the following manner. The FBI first installs Magic Lantern directly onto the suspect's computer by way of a Trojan horse virus, sent via email. Once installed, the software records every single keystroke that the suspect types. The FBI can then secretly break into the suspect's home to download the recorded data. This data is then analyzed to determine the suspect's encryption passwords. With these passwords, the FBI can then gain access to all of the suspect's encrypted data, without his knowledge.[22]

In 2006, a German attorney general sought a warrant from "the investigating judge of the federal court" that would authorize

---

[19] *Id.* (citation omitted) (internal quotation marks omitted).

[20] Council of the European Union, Draft Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime, No. 15569/08 of 11 Nov. 2008, at 5, *available at* http://register.consilium.europa.eu/pdf/en/08/st15/st15569.en08.pdf.

[21] *See, e.g.*, Wiebke Abel & Burkhard Schafer, *The German "Federal Trojan"—Challenges Between law and Technology*, TEUTAS L. & TECH. (Mar. 2, 2009, 17:48 GMT), *available at* http://www.teutas.it/societa-informazione/prova-elettronica/634-the-german-federal-trojan-challenges-.

[22] Ginger Vaudrey, *The Technology of National Security*, L. TECH., Jan. 1, 2004, *available at* 2004 WLNR 15265384 (footnotes omitted).

German police "to search a suspect's computer using an RFS [remote forensic tool]."[23] The application sought permission

> to investigate the data stored on the hard disk and the working memory of the computer. To accomplish this, a specifically designed computer program was to be planted on the suspect's computer without raising his suspicion. This program would then copy all data stored on the computer and subsequently transfer it back to the investigating authority for evaluation. In addition to files stored on the computer, access was also asked for email traffic and information about visited websites.[24]

When the judge declined to issue the warrant, the attorney general appealed to the federal court (the Bundesgerichtshof), which held that the warrant could not be issued because "no legal authorisation existed . . . under German law permitting the use of RFS tools in crime investigations by law enforcement agencies."[25] At around the same time, another German state adopted legislation that authorized the use of remote computer searches (or remote forensic tools), among other things.[26] A complaint was filed with the German Federal Constitutional Court (Bundesverfassungsgericht), challenging the constitutionality of this legislation.[27] On February 27, 2008, the Federal Constitutional Court held that it violated the German Constitution and was therefore unlawful and unenforceable.[28]

The "remote forensic tools" at issue in these cases apparently involved the use of Trojan Horse programs.[29] They seem to be at least one of the tools British police can utilize in carrying out

---

[23] Abel & Schafer, *supra* note 21; *see also German Police Seeks Legal Permission for Online House Search*, SPAMFIGHTER (Mar. 14, 2007), http://www.spamfighter.com/News-7911-German-Police-Seeks-Legal-Permission-for-Online-House-Search.htm.

[24] Abel & Schafer, *supra* note 21.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.* (The authors note that either computer viruses or Trojan Horse programs could be used, but they tend to emphasize the use of Trojan Horse programs.).

"intrusive surveillance" of certain suspects.[30] The Regulation of Investigatory Powers Act of 2000 (RIPA) gives certain officials the authority to authorize such surveillance.[31] An official cannot authorize intrusive surveillance unless he or she determines that it is necessary (i) "in the interests of national security"; (ii) to prevent or detect "serious crime"; or (iii) "in the interests of the economic well-being of the United Kingdom."[32] Intrusive surveillance can be authorized even if it "includes conduct outside the United Kingdom."[33]

RIPA defines intrusive surveillance as surveillance that is "carried out in relation to anything taking place on any residential premises" and "involves the presence of an individual on the premises . . . or is carried out by means of a surveillance device."[34] Surveillance that is carried out "by means of a surveillance device in relation to anything taking place on" residential premises or is carried out "without that device being present on the premises . . . is not intrusive unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises . . . ."[35]

According to the BBC, in 2009, the British Home Office "signed up to an EU strategy that 'encourages' police . . . to remotely access personal computers."[36] The story notes that British police already had the ability to conduct such searches and that a spokesman for the Association of Chief Police Officers told a reporter that "police were already carrying out a small number of these operations" each year.[37]

---

[30] *See, e.g.*, Flora Graham, *Police 'Encouraged' to Hack More*, BBC NEWS (Jan. 5, 2009, 18:04 GMT), http://news.bbc.co.uk/2/hi/7812353.stm (discussing the use of Trojan Horse programs).

[31] *See* Regulation of Investigatory Powers Act, 2000, c. 23, § 32(1) (Eng.) ("[T]he Secretary of State and each of the senior authorising officers shall have power to grant authorisations for the carrying out of intrusive surveillance.").

[32] *Id.* at c. 23, § 32(2)-(3).

[33] *Id.* at c. 23, § 27(3).

[34] *Id.* at c. 23, § 26(3).

[35] *Id.* at c. 23, § 26(5).

[36] Graham, *supra* note 30.

[37] *Id.*

I cannot find any information as to whether other members of the EU have followed Britain's lead and incorporated remote computer searches into their criminal procedure. My suspicion, and it is just that, is that most EU countries are not using remote computer searches because the authority to conduct such searches currently does not exist under their national laws.[38] Some of them may eventually decide to follow Britain's lead and adopt legislation that authorizes remote computer searches; others may side with Germany, concluding that such searches cannot be authorized under their foundational law. This brings us to the Fourth Amendment.

B. United States

The Fourth Amendment creates a right to be free from "unreasonable searches and seizures."[39] A Fourth Amendment violation occurs when there is (i) a search and/or seizure that (ii) is conducted by law enforcement[40] and (iii) is not "reasonable."[41]

In determining whether there has been a violation of the Fourth Amendment, courts begin not with whether the law enforcement conduct at issue was "reasonable," but with whether it resulted in a "search" and/or a "seizure."[42] A "search" violates a "reasonable expectation of privacy" in a place or a thing.[43] To have such an expectation of privacy, one must subjectively believe the area or object is private and society must accept that belief as objectively reasonable.[44] A "seizure" of someone's property occurs when "there is some meaningful interference with an individual's possessory interests in that property." [45] To be "reasonable," a search or seizure must be conducted pursuant to a warrant or pursuant to an applicable exception to the warrant requirement.[46]

---

[38] *See supra* note 20 and accompanying text.

[39] U.S. CONST. amend. IV.

[40] *See, e.g.*, United States v. Aldridge, 642 F.3d 537, 541 (7th Cir. 2011) ("The Fourth Amendment generally does not apply to searches and seizures by private parties, but it does apply if the private party is acting as a government agent.").

[41] In this Section, I am assuming the Fourth Amendment applies to law enforcement-initiated remote computer searches. Under current law, that (i) is true if the computer being searched is in the territorial United States or is owned by a U.S. citizen and (ii) is not true if the computer is outside the territorial United States and is not owned by a U.S. citizen. *See, e.g.*, United States v. Verdugo-Urquidez, 494 U.S. 259, 269-75 (1990). I, for one, suspect the second alternative is not a viable way to proceed, at least with regard to networked computer searches, because it can create tensions between nations. *See, e.g.*, Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. HIGH. TECH. L. 1, 21-23 (2004).

[42] *See, e.g.*, Boroian v. Mueller, 616 F.3d 60, 65 (1st Cir. 2010) (explaining that the threshold question to be resolved was whether there was a search or seizure; then having found that a search occurred, the court then determined its reasonableness).

[43] *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 211 (1986).

U.S.-initiated remote searches of the type authorized by RIPA, and sanctioned by the EU Council, will therefore violate the Fourth Amendment if they are (i) conducted by law enforcement, (ii) result in a search and/or seizure within the compass of the Fourth Amendment and (iii) are not "reasonable." I will assume, for the purposes of analysis, that the hypothesized remote searches under consideration in this Article *are* conducted by law enforcement officers, which brings us to the question of whether this activity results in a "search" and/or a "seizure."

C. Search

We will begin with searches. The use of a Trojan Horse program (or similar malware) to investigate the contents of someone's computer will constitute a "search" if the person had a reasonable expectation of privacy in the contents of that computer's hard drive. Not surprisingly, there seems to be no reported decisions that are precisely on point,[47] but courts have held that individuals have a reasonable expectation of privacy in the contents of their computer hard drives, unless they have taken actions that nullify that expectation.[48]

---

[44] *See, e.g.*, *Boroian*, 616 F.3d at 60, 65 ("whether a search or seizure had occurred" was the threshold question, to be resolved initially; having found that a search occurred, the court then determined its reasonableness); *see also* Katz v. United States, 389 U.S. 347, 351 (1967).

[45] Soldal v. Cook Cnty., 506 U.S. 56, 61 (1992) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)) (internal quotation marks omitted).

[46] *See, e.g.*, United States v. Butler, 405 Fed. App'x 652, 655 (3d Cir. 2010).

[47] In *United States v. Steiger*, the defendant moved to suppress evidence obtained from his computer, arguing that the search warrant for the computer was invalid "because it was based in part on information from an anonymous source who hacked into his computer." 318 F.3d 1039, 1045 (11th Cir. 2003). In communications to law enforcement, the anonymous source claimed to have used a Trojan Horse program to "enter into Steiger's computer via the Internet" and download evidence which he then sent to police. *Id.* at 1043-45. The Eleventh Circuit held that suppression was not in order because the anonymous source "acted at all material times as a private individual," and the Fourth Amendment does not apply to the conduct of private

They have analogized a computer's hard drive to a "container," and found that absent countervailing circumstances,[49] hard drives are accorded protection "similar to the protection [the Fourth Amendment] affords a person's closed containers and closed personal effects."[50] Since individuals have a presumptively reasonable expectation of privacy in closed containers,[51] it follows that they have a reasonable expectation of privacy in computer "containers," unless they have taken actions that diminish or defeat that expectation of privacy.

In analyzing the potential Fourth Amendment implications of remote computer searches, I shall assume such searches target computers located in an individual's home or office. I make that assumption because it adds a dimension to the analysis.[52]

---

citizens. *Id.* at 1045; *accord* United States v. Jarrett, 338 F.3d 339, 346-47 (4th Cir. 2003).

[48] *See, e.g.*, United States v. Leiske, No. 08-CR-453-KI, 2011 WL 3205308, at *6 (D. Or. July 27, 2011); United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998); Commonwealth v. Cormier, No. 09-1365, 2011 WL 3450643, at *3-4 (Mass. Super. Ct. June 27, 2011).

[49] For what constitutes such circumstances, see *infra* notes 58-60 and accompanying text.

[50] United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998); *see, e.g.*, United States v. Peden, No. CR. 06-0300 WBS, 2007 WL 2318977, at *3 (E.D. Cal. Aug. 13, 2007) ("'A person has an expectation of privacy in his or her private, closed containers'" which "[u]ndoubtedly . . . extends to personal computers in one's home . . . ." (quoting United States v. Fultz, 146 F.3d 1102, 1105 (9th Cir. 1993))); People v. Carratu, 755 N.Y.S.2d 800, 807 (N.Y. Sup. Ct. 2003) ("By placing data in files on the hard drive of his computer, defendant manifested a reasonable expectation of privacy in the contents of those files."); Brackens v. State, 312 S.W.3d 831, 837 (Tex. Ct. App. 2009) ("The Fourth Amendment protection afforded to closed computer files and hard drives is similar to the protection afforded to a person's closed containers and closed personal effects."); *see also* United States v. Payton, 573 F.3d 859, 862 (9th Cir. 2009) ("Searches of computers . . . often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."); United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) ("[C]omputers should fall into the same category as suitcases, footlockers, or other personal items that command a high degree of privacy.").

[51] *See, e.g.*, United States v. Ross, 456 U.S. 798, 822-23 (1982); United States v. Villarreal, 963 F.2d 770, 773-74 (5th Cir. 1992).

[52] I also utilize this assumption to simplify the empirical aspects of the analysis; the conclusions derived from the home-office analysis should apply with equal force to

Traditionally, to access data on such a computer, police officers must (i) first enter the computer owner's home or office and (ii) then "enter" the computer itself. A traditional search of a computer located in a home or office involves two entries (one into the home or office, the other into the computer), each of which must be reasonable under the Fourth Amendment.

I shall also assume, again for the purposes of this analysis, that the computer owner has a reasonable expectation of privacy in her home or office,[53] which means the officers' entry into the premises constitutes a search under the Fourth Amendment. For such an entry to be lawful, it would have to be authorized either by a search warrant or by an applicable exception to the warrant requirement.[54] The same is true of the officers' "entry" into the computer. As such, I shall assume for the purposes of analysis that their accessing the contents of the computer-as-closed-container violates a reasonable expectation of privacy (again, absent countervailing circumstances)[55] and therefore must be authorized by a warrant or an exception to the warrant requirement.[56]

The analysis above applies to physical searches of someone's home or office and of a computer located in that home or office. Does it also apply to remote searches of computers located in a

---

remote searches targeting computers that are located in places other than the suspect's own home or office, e.g., in a home that belongs to someone other than the suspect or in a public place, such as an airport or a Starbucks. While computers located in someone's home or office may be entitled to a heightened level of Fourth Amendment protection, individuals do not necessarily surrender a reasonable expectation of privacy in a closed container by taking it with them into publicly accessible areas. *See, e.g.*, Bond v. United States, 529 U.S. 334, 336-37 (2000); *see also* United States v. Astley-Teixera, No. ACM 35161, 2003 WL 22495794, at *7 (A.F. Ct. Crim. App. Oct. 21, 2003) (defendant had a reasonable expectation of privacy in his laptop, which he left "open, powered-on, and not password protected" in his dorm room).

[53] Absent countervailing circumstances, individuals enjoy a reasonable expectation of privacy in their own homes. *See, e.g.*, Payton v. New York, 445 U.S. 573, 589-90 (1980). And, depending on the circumstances, individuals may have a reasonable expectation of privacy in their offices. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 715-17 (1987).

[54] *See supra* note 47 and accompanying text.

[55] For what constitutes such circumstances, see *infra* notes 58-60 and accompanying text.

[56] *See, e.g.*, United States v. Hanson, No. CR 09-00946 JSW, 2010 WL 2231796, at *3 (N.D. Cal. June 2, 2010).

home or office? To resolve that question, we need to analyze several distinct issues, the first of which is whether a remote computer search involves a physical "entry" of the home or office in which the computer is located. Literally, it does not; the officers who examine the contents of the computer's hard drive do not physically cross the threshold of the home or office in which it is located.[57] Logically, then, a remote computer search is a more circumscribed Fourth Amendment event than the traditional computer searches outlined above; in a remote search, the officers access the contents of the computer's hard drive but not the premises on which it is located. Arguably, they would not need to obtain a warrant to search those premises in order to conduct the remote search of the computer; since there is no physical entry into the home or office, it seems the only potential Fourth Amendment event is the exploration of the computer.[58]

As we saw earlier, absent countervailing circumstances, individuals will have a reasonable expectation of privacy in their computers—especially if they are located in generally private areas, such as a home or office—because computers are considered to be "closed containers."[59] Computers, though, differ from traditional containers in one notable respect: They are linked to the Internet through a network (which, of course, is essential if our hypothesized investigators are to conduct remote computer searches). To access traditional containers, law enforcement officers must cross the threshold of the suspect's home or office in order to locate and access the contents of the container; to access a networked computer, officers can exploit the fact that it is online. That adds a dimension to the analysis; the computer-container essentially offers officers a direct portal into the data it contains, a point of "entry" they can exploit without affecting any physical entry into Fourth Amendment-protected premises.

---

[57] *See supra* note 53 and accompanying text.

[58] United States v. Martinez-Fuerte, 428 U.S. 543, 561 (1976). The absence of "[p]hysical entry of the home" in this scenario removes the "chief evil against which the . . . Fourth Amendment is directed." United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297, 313 (1972). The text below examines the related issue of whether the officers' copying data from the computer constitutes a Fourth Amendment seizure that must also be authorized by a warrant or an exception to the warrant requirement.

[59] *See supra* notes 49-50 and accompanying text.

Is the availability of that portal sufficient, in and of itself, to negate the reasonable expectation of privacy individuals would otherwise enjoy in their computer-containers? An argument can be made that it does: A number of courts have found that one who installs and enables "peer-to-peer file sharing on his computer, thereby giving anyone with internet access the ability to gain entrance to his computer," has "no reasonable expectation of privacy" in the contents of that computer.[60] These courts have held, therefore, that it is not a violation of the Fourth Amendment for a law enforcement officer to utilize file-sharing software to locate and download files designated for sharing from someone's computer, even if that computer was in the suspect's home.[61]

Prosecutors and law enforcement officers might argue that the same premise applies to computer users who link their computers to the Internet. As we saw earlier, to have a cognizable Fourth Amendment expectation of privacy in a place or thing, one must subjectively believe the place or thing is private, and society must accept that belief as objectively reasonable.[62] Courts have found that those who use file-sharing software do not have such an expectation of privacy as to the files they designate for sharing even if they personally believe the files are private because society does not accept that belief as objectively reasonable.[63] These courts have, at least implicitly, found that the use of file-sharing software defeats a Fourth Amendment expectation of privacy only as to the files the person has made available for sharing.[64]

---

[60] United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); *see also* United States v. Stults, 575 F.3d 834, 842-43 (8th Cir. 2009). The premise is that by installing and using file-sharing software, the person "knowingly exposes to the public" information that would otherwise be protected by the Fourth Amendment. United States v. Norman, No. 2:09-CR-118-WKW, 2010 WL 3825606, at *4 (M.D. Ala. July 6, 2010), report and recommendation accepted in part, rejected in part, No. 2:09cr118-WKW, 2010 WL 3825601 (M.D. Ala. July 6, 2010).

[61] *See, e.g.*, United States v. Ladeau, No. 09-40021-FDS, 2010 WL 1427523, at *3-6 (D. Mass. Apr. 7, 2010).

[62] *See supra* note 44 and accompanying text.

[63] *See, e.g.*, United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008).

In other words, they have not held that the mere act of linking a computer to a network (and thereby to the Internet) defeats the owner's reasonable expectation of privacy in the contents of the computer itself. Indeed, at least one court has held to the contrary.[65] That, I submit, is the correct way to approach Fourth Amendment privacy with regard to computers that are (merely) linked to a network. I believe this approach is consistent with the Supreme Court's decision in *Katz v. United States*.[66] The *Katz* Court held that it was a Fourth Amendment search for law enforcement officers to use "an electronic listening and recording device" to access and capture the contents of calls he made while in a public telephone booth.[67] The Court found that Charles Katz had a reasonable expectation of privacy in the contents of the calls because he subjectively believed they were private and society accepted his belief as objectively reasonable.[68]

It seems to me that the computer user whose hard drive is invaded by a law enforcement Trojan Horse program is in a situation functionally analogous to the one Katz found himself in. Both utilize methods of "online" communication that rely on technology; both assume their "content" is private—the computer user because she is on her computer in her home or office, and Katz because he was in a phone booth the door of which was securely closed.[69] In neither scenario can law enforcement access the content in question without utilizing dedicated technology that lets the officers invade a private enclave (hard drive, phone booth) in a fashion a reasonable person would not expect. In neither scenario do we have the target of that invasion engaging in conduct that abrogates a Fourth Amendment expectation of privacy in the area that is invaded, i.e., neither Katz nor our hypothetical computer user knowingly engaged in conduct that exposed their respective content to the public, and thereby to law enforcement.

---

[64] *Id.* ("Ganoe thus opened up his download folder to the world, including Agent Rochford."); *see also* United States v. Borowy, 577 F. Supp. 2d 1133, 1136 (D. Nev. 2008).

[65] *See* United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) ("[T]he mere act of accessing a network does not in itself extinguish privacy expectations . . . .").

[66] 389 U.S. 347 (1967).

[67] *Id.* at 348, 359.

[68] *Id.* at 351-59*; see also id.* at 360-62 (Harlan, J., concurring).

[69] The scenarios differ in one respect: In *Katz*, the officers intercepted the contents of Katz's phone conversations as they occurred; in our hypothesized scenario, officers access content that is stored on the computer user's hard drive. I do not see this distinction as particularly significant for the present analysis because I think it is purely the product of empirical circumstance: Since phone conversations are dynamic, the only ways the officers could obtain the contents of Katz's calls was to record them as they occurred. Computer-stored content, on the other hand, is relatively stable,

I will, therefore, assume that law enforcement's using a Trojan Horse program to surreptitiously obtain content from the hard drive of a computer in someone's home or office constitutes a Fourth Amendment search and must be authorized either by a search warrant or by an exception to the warrant requirement. That, of course, only generates additional questions: What should such a warrant contain? How is it to be executed? What exceptions might substitute for a warrant in this context?

I will address those issues in a moment. Before I proceed with that analysis, I want to briefly address the issue as to whether law enforcement's using a Trojan Horse program to download content from someone's hard drive constitutes a "seizure" under the Fourth Amendment.

D. Seizure

As I noted earlier, a seizure of property occurs when law enforcement conduct "meaningfully" interferes with the owner's possession and use of that property.[70] In this analysis, I am assuming officers use a Trojan Horse program to access the contents of an unwary computer user's hard drive (search), to copy

---

regardless of its nature; a hard drive can store user-generated content, content the user downloaded from the Internet and emails the user has exchanged with others. *See, e.g.*, Lincoln Spector, *Where Does Windows Live Mail Store My Mail?*, PC WORLD (Apr. 8, 2011, 7:11 AM), http://www.pcworld.com/article/223781/where_does_windows_live_mail_store_my_mail.html. I do not see the type of information being accessed as dispositive; what matters is that, in both scenarios, officers use surreptitious communications technology to obtain content they otherwise would not be able to obtain except by physically invading a Fourth Amendment space, e.g., the computer user's home/office or Katz's phone booth.

[70] *See supra* note 45 and accompanying text.

data from that hard drive and to retrieve the copy for the officers' professional use. To constitute a seizure, the acts of copying the data and retrieving the copy would have to "meaningfully" interfere with the owner of the data's ability to possess and use it.

As I have explained elsewhere, I believe copying data is a seizure, albeit a seizure that differs in one important respect from traditional seizures of property.[71] In a traditional seizure of physical property, an officer prevents the owner from accessing that property for a brief period of time (temporary detention) or permanently (by taking the property with no intention of returning it to the owner). Either type of physical seizure is a zero-sum event, i.e., the possession and use of the property passes wholly from the owner to the officer for the duration of the seizure. Copying data is, as I have argued elsewhere,[72] a non-zero-sum seizure, i.e., there is a less than absolute interference with the owner's possession and use of the property.

Assume FBI Agent John Doe uses a Trojan Horse program to access the hard drive of Mary Smith's computer, which is in her home. After searching the contents of the hard drive, Doe copies certain files and downloads the copies to his hard drive. Smith still has the data, but she no longer has exclusive possession of it; that, I argue, results in a meaningful interference with her possession of that property.[73]

I analogize this type of copying to copying that is prosecuted as theft. In 1993, Randal Schwartz was prosecuted for theft of proprietary information.[74] The prosecution was based on Schwartz's copying a computer password file that belonged to the

---

[71] *See* Susan W. Brenner & Barbara S. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 106-13 (2002); Susan W. Brenner, *Copying as Search and Seizure*, CYB3RCRIM3 (Oct. 26, 2009, 8:32 AM) [hereinafter Brenner, *Copying*], http://cyb3rcrim3.blogspot.com/2009/10/copying-as-search-and-seizure.html; Susan W. Brenner, *Seizure*, CYB3RCRIM3 (Feb. 19, 2006, 2:35 PM), http://cyb3rcrim3.blogspot.com/2006/02/seizure.html.

[72] *See* Brenner, *Copying*, *supra* note 71.

[73] *See* Brenner, *Copying*, *supra* note 71. For a case that reached a similar conclusion, see *United States v. Jefferson*, 571 F. Supp. 2d 696, 703-04 (E.D. Va. 2008) (photographing information constituted a seizure).

[74] State v. Schwartz, 21 P.3d 1128, 1131, 1135 (Or. Ct. App. 2001).

Intel Corporation, which had employed him as a contractor.[75] After being convicted, Schwartz appealed, arguing, in part, that he could not be convicted of "theft" because while he copied the password file, "the file and passwords remained on Intel's computers."[76] The prosecution argued, in response, that the "loss of exclusive possession of the passwords . . . [was] sufficient to constitute theft." [77] After parsing the meaning of "theft," the court of appeals concluded that it could encompass non-zero-sum appropriations of intangible property, and therefore upheld Schwartz's conviction.[78]

This court, therefore—at least implicitly—recognized that copying data constitutes a meaningful interference with the owner's possession and use of that digital property, even though it does not wholly deprive the owner of the possession of that property. If we extrapolate that principle to the Fourth Amendment context, I believe we necessarily conclude that copying is a non-zero-sum seizure.

For the purposes of this analysis, then, I will assume that law enforcement's copying data constitutes a seizure. That brings us to the next issue—ensuring that the use of a Trojan Horse program to carry out digital searches and seizures is reasonable.

E. Trojan Horse Warrants

A Trojan Horse warrant would have to be supported by probable cause, [79] i.e., would have to be based on facts and circumstances that are "sufficient . . . to warrant a man of reasonable caution in the belief that" evidence of a crime will be found in the computer to be searched.[80] Establishing probable cause to conduct a remote computer search should not be particularly difficult. In *United States v. Gitarts*,[81] the FBI developed the information needed to establish probable cause for a "remote" search of a computer server by working with a confidential informant and obtaining information from other credible sources.[82] Officers have also used information concerning a suspect's use of file-sharing software to establish the probable cause needed to obtain a warrant to search a computer for child pornography.[83]

---

[75] *Id.* at 1130-31.

[76] *Id.* at 1136.

[77] *Id.* at 1137.

[78] *See id.*

[79] *See* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . .").

[80] Brinegar v. United States, 338 U.S. 160, 175-76 (1949) (quoting Carroll v. United States, 267 U.S. 132, 162 (1925)) (internal quotation marks omitted); *see, e.g.*, Ornelas v. United States, 517 U.S. 690 (1996) (standard enunciated above constitutes probable cause to search for evidence).

The warrant would also have to particularly describe "the place to be searched, and the . . . things to be seized." [84] The "place" to be searched is the suspect's computer. When officers obtain a warrant to conduct a traditional search of a suspect's computer, they may particularly describe that specific computer[85] or they may seek a warrant to the computer or computer to be found at the premises where the search is to be conducted. Since computers are regarded as "containers," courts have held that a warrant satisfies the Fourth Amendment if it authorizes a search of a computer or computers. Officers might employ these approaches in obtaining a warrant for a Trojan Horse search, or they might proceed somewhat differently. They might "particularly describe" the "place" to be searched as the computer that is using a specific internet protocol (IP) address.[86]

The "things to be seized" would consist of computer data. The warrant would have to describe the things to be searched for and seized with some specificity, which would probably be done by specifying the *type* of data the officers are authorized to seek and acquire. Courts have held that the Fourth Amendment's particularity requirement is satisfied if officers "describe with particularity the objects of their search," e.g., specify they are searching for evidence of child pornography or evidence of drug dealing and seek authorization to seek that evidence if and when they find it.[87] So, a Trojan Horse warrant might specify that the malware is to be used to search a computer remotely for evidence of terrorist activity or child pornography.[88]

---

[81] 341 F. App'x 935 (4th Cir. 2009).

[82] *See id.* at 937-39. The prosecution was brought in Virginia; the server was in Texas. *Id.* at 939.

[83] *See, e.g.*, Panuski v. State, No. 88, 2010, 2010 WL 3398945, at *1 (Del. Aug. 30, 2010); State of Delware's Answering Brief at *3-4, Panuski v. State, No. 88, 2010, 2010 WL 2565705 (Del. June 14, 2010).

[84] U.S. CONST. amend. IV.

[85] *See, e.g.*, United States v. Voraveth, Crim. No. 07-419 DWF/AJB, 2008 WL 4287293, at *3 (D. Minn. July 1, 2008).

[86] *See, e.g.*, United States v. Rosetter, Crim. No. 10-83 (JNE/JSM), 2010 WL 5184991, at *13-14 (D. Minn. Oct. 1, 2010); United States v. Klynsma, No. CR. 08-50145-RHB, 2009 WL 3147790, at *7 (D.S.D. Sept. 29, 2009); *see generally* Johnson v. Microsoft Corp., No. C06-0900RAJ, 2009 WL 1794400, at *3 (W.D. Wash. June 23, 2009) ("When a person uses a computer to accesses the Internet, the computer is assigned an IP address by the user's Internet service provider.").

That brings us to executing the warrant. Given the nature of the search, it seems obvious that the officers who remotely access the computer will not knock and announce their intention to "enter" it to conduct the search.[89] Although the Supreme Court has held that knocking and announcing is an element of Fourth Amendment analysis,[90] officers are not required to knock and announce their presence and intentions if they have reasonable suspicion that doing so would be dangerous or would inhibit the investigation by giving a suspect the opportunity to destroy evidence.[91] It is highly unlikely that officers initiating a remote search of a suspect's computer would reasonably fear physical injury to themselves, but they might very well have reason to suspect that announcing their intentions prior to commencing the search could result in the destruction of evidence. If the officers charged with executing a specific Trojan Horse warrant could articulate the necessary reasonable suspicion, that should eliminate the need for virtual knocking and announcing; the process would, of course, proceed on a case-by-case basis.

---

[87] United States v. Welch, 291 F. App'x 193, 205 (10th Cir. 2008); *see also* United States v. Stabile, 633 F.3d 219, 237-39 (3d Cir. 2011); United States v. Blake, No. 1:08-cr-0284 OWW, 2010 WL 702958, at *3 (E.D. Cal. Feb. 25, 2010).

[88] Two authors have suggested that the Trojan Horse program might be configured so that it automatically avoids data that is not within the scope of the Trojan Horse warrant:

> If a police Trojan has accessed a suspect's computer and is searching the hard-drive for relevant data, it should "understand" that certain types of . . . private data such as health records, is protected by the constitutional rights of the suspect, and is therefore "inaccessible" by the police. This should trigger a corresponding "disability" by the agent to collect information unless there is also a superseding "power" that overrules the suspect's constitutional rights on this occasion, and allows the exceptional violation.

Abel & Schafer, *supra* note 21.

[89] *See, e.g.*, Wilson v. Arkansas, 514 U.S. 927, 930 (1995) (common-law knock-and-announce principle is part of Fourth Amendment reasonableness analysis).

[90] *Id.*

[91] *See* Richards v. Wisconsin, 520 U.S. 385, 394-95 (1997).

The Fourth Amendment does not specify a time period within which warrants must be executed, but the federal system and most, if not all, states do this with court rules or statutes.[92] Under Rule 41 of the Federal Rules of Criminal Procedure, warrants that authorize copying "electronically stored information" are executed in a timely fashion if the information is copied within the specified time period.[93] This is a reasonable approach for the execution of what I am referring to as traditional computer searches, but it may not be adequate for Trojan Horse warrants.

Rule 41 and the comparable state provisions all assume that the "execution" of a warrant is a single, unitary event, analogous to officers' seizing stolen televisions from a suspect's home. That assumption is almost certainly not valid for Trojan Horse warrants because they are executed, not by human beings, but by semi-autonomous software programs.[94] Since Trojan Horse programs "can work autonomously without the direct intervention of a human controller, their search is not limited to a specific time period. Hence, they are (potentially) ubiquitous and 'always on.'"[95] Court rules and statutes could address this issue by requiring (i) that the Trojan Horse program be deleted from the target computer once the authorized search had been completed or (ii) that officers disable the program, thereby preventing it from continuing to conduct searches on the target computer.[96]

---

[92] *See, e.g.*, FED. R. CRIM. P. 41(e)(2)(A)(i) ("14 days"); *see also* ALA. CODE § 15-5-12 (1995); IDAHO CODE ANN. § 19-4412 (2004); W. VA. CODE ANN. § 62-1A-4 (LexisNexis 2010); 68 AM. JUR. 2D *Searches and Seizures* § 302 (2010).

[93] *See* FED. R. CRIM. P. 41(e)(2)(B). The rule is intended to clarify that a warrant for digital evidence is "executed" when the evidence is seized, not when the review of the evidence is complete. *Id.*

[94] *See* Abel & Schafer, *supra* note 21.

[95] *Id.*

[96] I am assuming, for the purposes of analysis, that the execution of a Trojan Horse warrant only targets content that was stored on the computer when the software was installed on it. That is, I am assuming the Trojan Horse program does *not* intercept content as it arrives and is stored on the computer. Intercepting content, especially communications such as e-mail, would implicate the heightened requirements of Title III and analogous state wiretap statutes. *See, e.g.*, U.S. Dep't of Justice Computer Crime and Intellectual Prop. Sec., *Searching and Seizing Computers and Obtaining*

I need to address one final issue that could complicate the execution of a Trojan Horse warrant before I address the use of exceptions to the warrant requirement as an alternative way of satisfying Fourth Amendment requirements for remote computer searches. That issue is the unique problem posed by antivirus software.

As one article notes, a police Trojan Horse program is "from a design perspective nothing else than a piece of malware," and antivirus software is designed to detect and deflect malware.[97] "The problem is that any government-designed [Trojan Horse program] features these attributes and may therefore be detected by anti-virus products because they are not able to differentiate between a" law enforcement program and malware.[98] Commercial antivirus software installed on the target computer could therefore interfere with, or even block, the law enforcement Trojan Horse's ability to conduct the search (and seizure) authorized by the warrant. Unless law enforcement could create (or acquire) Trojan Horse programs that were not detected by commercial antivirus software, the solution to this problem seems to lie in law enforcement's persuading antivirus companies to "deliberately not detect" law enforcement Trojan Horse programs or disable their antivirus software if and when such a program were installed pursuant to a warrant.[99] One problem with this solution is that it could cause consumers to lose trust in the products created and marketed by the cooperating antivirus vendors; another problem is the "companies that [create] antivirus software are not necessarily in the same jurisdiction as the suspect" whose computer is to be searched, which means the relevant antivirus

---

Electronic Evidence in Criminal Investigations: Electronic Surveillance in Communications Networks, CYBERCRIME.GOV (2009), http://www.cybercrime.gov/ssmanual/04ssma.html; *see also* State v. Poling, 938 N.E.2d 1118, 1124 (Hocking Cnty. Mun. Ct. 2010).

[97] Abel & Schafer, *supra* note 21.

[98] *Id.*

[99] *Id.* There are federal and state statutes that authorize law enforcement officers to utilize the assistance of private citizens in executing warrants. *See, e.g.*, 18 U.S.C. § 3105 (2006).

company or companies might have little, if any, incentive to cooperate with U.S. law enforcement.[100]

F. Exceptions

Since I suspect many of the exceptions to the Fourth Amendment's warrant requirement—such as search incident to arrest, inventory searches, consent searches, the vehicle exception and administrative searches—are likely to have little, if any, applicability to remote computer searches, I am only going to address two exceptions: one, which is likely to apply, and the other, which is not likely to apply in this context.

The exception that is likely to apply is the exigent circumstances exception. The exception allows officers to enter premises without a warrant to conduct a search if they have probable cause to conduct the search and if an exigency justifies entering without a warrant.[101] Courts have recognized four types of exigency that justify such an entry: (1) the need to prevent physical harm to someone inside the premises; (2) the need to prevent the imminent destruction of evidence; (3) hot pursuit of a fleeing suspect; and (4) the need to prevent the escape of a suspect.[102] I, for one, do not believe three of these exigencies could apply to remote computer searches; the only exigency I see that could apply here is the need to prevent the destruction of evidence.

There is, indeed, precedent for applying this exigency to a remote computer search. In *United States v. Gorshkov*,[103] FBI agents "logged onto" a computer in Russia that was used by a cybercrime suspect whom they had arrested.[104] The agents downloaded data from the Russian computer without first obtaining a warrant; the government later used the data in its prosecution of the suspect—Vasiliy Gorshkov.[105] Gorshkov moved to suppress the data, claiming the search of his computer violated the Fourth Amendment.[106] The prosecution argued that the search was justified by the exigent circumstances exception because the "agents had probable cause to believe that the Russian computers contained evidence of crimes" and "good reason to fear that if they did not copy the data," Gorshkov's "coconspirators would destroy" it.[107] The district court agreed with the prosecution, and denied Gorshkov's motion to suppress.[108] I can see the same theory being used to justify remote computer searches, as long as the officers who are charged with carrying out the search can point to specific facts that reasonably led them to believe they needed to act without first obtaining a warrant.

---

[100] Abel & Schafer, *supra* note 21.

[101] *See, e.g.*, United States v. Struckman, 603 F.3d 731, 739 (9th Cir. 2010).

[102] *Id.* at 743.

[103] No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

[104] *See id.* at *1.

[105] *Id.*

The exception I do not believe can apply in this context is not really an exception at all. As the Supreme Court noted in *Texas v. Brown*,[109] the plain view doctrine "is perhaps better understood . . . not as an . . . 'exception' to the Warrant Clause, but . . . as an extension of whatever the prior justification for an officer's 'access to an object' may be."[110] Under the plain view doctrine, "if police are lawfully in a position from which they view an object, if its incriminating character is immediately apparent, and if the officers have a lawful right of access to the object, they may seize it without a warrant."[111] The doctrine only justifies a seizure; it cannot justify a search.[112]

Courts have upheld the applicability of the plain view doctrine in police-initiated physical searches of computers and hard drives.[113] Typically, courts uphold the applicability of the plain view doctrine when an officer is searching a computer's hard drive pursuant to a search warrant, observes data whose "incriminating character. . . [is] 'immediately apparent,'" and seizes the data.[114] I do not see how this dynamic can apply in remote computer searches because here the search is conducted, not by a human being, but by semi-autonomous software.[115] There is, therefore, no individual to observe data the incriminating character of which is immediately apparent to him or her; absent that, how can the plain view doctrine apply?

---

[106] *Id.*

[107] *Id.* at *4.

[108] *Id.*

[109] 460 U.S. 730 (1983).

[110] *Id.* at 738-39.

[111] Minnesota v. Dickerson, 508 U.S. 366, 375 (1993).

[112] *See id.*

[113] *See, e.g.*, United States v. Stabile, 633 F.3d 219, 240-41 (3d Cir. 2011).

[114] *Id.* at 241.

Some might argue that software could be configured so the Trojan Horse program being used in the search could, like a human investigator, recognize data that was not within the scope of the warrant but that was clearly incriminating for different reasons, and that it would be reasonable to allow the software to expand its activities by merely seizing this evidence, as well. Aside from anything else, I, for one, would be reluctant to allow this expansion of the plain view doctrine for fear that it might lead to manipulations that deliberately and impermissibly expanded the scope of a Trojan Horse warrant.

II. VIRTUAL FORCE?

In November 2010, WikiLeaks, a "whistleblower" organization used the Internet to publish "[a] cache of a quarter-million confidential" diplomatic cables from 274 United States embassies.[116] WikiLeaks apparently received the cables from Bradley Manning, a U.S. Army soldier who allegedly downloaded them from SIPRNet, the Secret Internet Protocol Router Network used by the U.S. Department of Defense and Department of State.[117]

As WikiLeaks began releasing the cables, the computer servers that hosted its website were attacked by unknown sources, taking the website offline.[118] The attack took the form of a Distributed Denial of Service (DDoS) attack,[119] which overwhelms a website with so much traffic it becomes "unavailable to its intended users."[120] A DDoS attack saturates the server hosting a website "with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable." [121] Cybercriminals often use DDoS attacks to extort money; the extortionists use a DDoS attack to shut down a commercial website, such as a casino, then demand money to refrain from repeating the attack.[122]

---

[115] *See* Abel & Schafer, *supra* note 21.

[116] Scott Shane & Andrew W. Lehren, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES, Nov. 29, 2010, at A1, *available at* http://www.nytimes.com/2010/11/29/world/29cables.html.

[117] *See, e.g.*, Kim Zetter, *Army: Manning Snuck 'Data-Mining' Software Onto Secret Network*, WIRED (Apr. 4, 2011, 4:28 PM), *available at* http://www.wired.com/threatlevel/2011/04/manning-data-mining/.

[118] *See, e.g.*, *WikiLeaks Under Denial of Service Attack (DDoS)*, SECURITY WEEK (Nov. 28, 2010), http://www.securityweek.com/wikileaks-under-denial-service-attack-ddos.

[119] *Id.* ("[I]ts Web site is currently under mass distributed denial of service attack.").

The DDoS attack against WikiLeaks was not designed to further an extortion attempt. It was apparently intended to impede WikiLeaks' ability to release the cables Manning allegedly leaked, which led some to suggest that the U.S. government was responsible for them. [123] In early December, a "Pentagon spokesman" said the U.S. Cyber Command[124] "had the means to shut down WikiLeaks but . . . policy makers thought it 'not appropriate' because [the] threat [was] not 'of high consequence.'"[125]

---

[120] Jason Fritz, *How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness*, 8 CULTURE MANDALA 28, 53 (2008), *available at* http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm.

[121] U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION STAFF REPORT: THE NATIONAL SECURITY IMPLICATIONS OF INVESTMENTS AND PRODUCTS FROM THE PEOPLE'S REPUBLIC OF CHINA IN THE TELECOMMUNICATIONS SECTOR 82-83 (2011), *available at* http://www.uscc.gov/RFP/2011/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf.

[122] *See, e.g.*, John Leyden, *Korean Web Host Charged Over DDoS Extortion Scam*, REGISTER (Jan. 11, 2011, 12:28 GMT), http://www.theregister.co.uk/2011/01/11/korean_gambling_ddos_extortion_charges/.

[123] *See, e.g.*, Rob Korczak, *DDoS Attack on Wikileaks Failed to Stop Cablegate Leaks*, ASSOCIATED CONTENT (Nov. 28, 2010), http://www.associatedcontent.com/article/6064458/ddos_attack_on_wikileaks_failed_to_pg2.html?cat=15.

[124] The U.S. Cyber Command is a "sub-unified command subordinate to United States Strategic Command" that "centralizes direction of cyberspace operations," including offensive and defensive cyber-attacks. *U. S. Cyber Command*, UNITED STATES STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/cyber_command/ (last visited Feb. 28, 2012).

[125] James Joyner, *Pentagon: We Could Have Taken WikiLeaks Down*, OUTSIDE THE BELTWAY (Dec. 2, 2010), http://www.outsidethebeltway.com/pentagon-we-could-have-taken-wikileaks-down/. Around the same time, a "self-proclaimed 'hacktivist'" said he was responsible for the attack. Paul McDougall, *"Hacktivist" Claims Credit for WikiLeaks Attack*, INFORMATIONWEEK (Dec. 1, 2010, 8:00 AM),

When I read about the WikiLeaks DDoS attack, it occurred to me that it might be coming from the U.S. government, which clearly had the motive and means to carry out such an assault. The idea of using DDoS attacks to shut down websites that host objectionable content is far from new: In 2001, then German Interior Minister Otto Schily "suggested that the German government" might use DDoS attacks "to shut down some sites based in the United States."[126] The sites in question were neo-Nazi websites, which provide content that is easily accessible in Germany; disseminating such content is a crime under German law.[127] Germany, of course, never launched such attacks; I suspect Schily's suggestion was simply the product of an understandable frustration at being unable to persuade U.S. authorities to block the sites or otherwise prevent the content they provide from being available to German citizens.

While the U.S. government may not have been responsible for the DDoS attack against WikiLeaks, this does not mean it cannot, and will not, use such attacks in the future. If the remarks of the "Pentagon spokesman" were reported correctly, the U.S. did not launch a DDoS attack against WikiLeaks because it did not deem the "harm" being inflicted by the release of the confidential (but not classified) cables significant enough to warrant such a response. It is therefore logical to infer that the United States *will* use a DDoS attack—or DDos attacks—to respond to the release of information or to other activity that inflicts "harm" significant enough to justify such a response. The likelihood of the United States resorting to DDoS attacks probably increases in proportion to the egregiousness of the "harm" being inflicted and the unavailability of alternative remedies.

The U.S. government's use of DDoS attacks to respond to "harm" being inflicted by online activity raises a number of legal issues, including the possibility that the attacks could be

---

http://www.informationweek.com/news/cloud-computing/software/showArticle.jhtml?articleID=228400244.

[126] Steve Kettmann, *Nebraksa Neo-Nazi Irks German Pol*, WIRED (Jan. 10, 2002), http://www.wired.com/politics/law/news/2002/01/49566.

[127] *See* STRAFGESETZBUCH [StGB] [PENAL CODE] Nov. 13, 1998, BUNDESGESETZBLATT [BGBL. I] 3322, as amended, §§ 86 & 86a (Ger.).

construed as offensive cyber-warfare.[128] That, however, is not the only possibility: Since warfare has traditionally involved a conflict between nation-states, the U.S. could argue that its using DDoS attacks against a civilian target constituted an exercise of law enforcement authority, rather than a military assault on another sovereign.[129] This argument is the product of what seems to have been a heretofore unrealized possibility: that a nation-state could use what in other circumstances would be military force against a civilian or group of civilians, the activities of which were in no way sponsored by or associated with the interests of a nation-state.[130]

If the use of DDoS attacks against a civilian target—a website that is disseminating classified information or bombarding U.S. targets with computer worms or other damaging data—represented an exercise of domestic law enforcement authority, the use of such attacks would have to comport with the requirements of the Fourth Amendment. That is the issue—the only issue—I will address in the remainder of this Article.[131]

To analyze the Fourth Amendment implications of using DDoS attacks against a civilian target that is located outside the United States, we need to outline a scenario that can provide the basis of our analysis and parse the Fourth Amendment principles that would be implicated by such an attack. For the scenario, we will use a variation of the WikiLeaks case. We will assume that a website located in another country is inflicting "harm" in the United States; the "harm" could involve releasing classified information, but I prefer to focus on something more concrete. We will assume that (i) the external site is attacking U.S. financial institutions; (ii) the attacks erode the stability of the institutions by interfering with normal operations and siphoning money from them; and (iii) the U.S. has asked the government of the country in which the site is located for assistance in stopping the attacks and apprehending the perpetrators, but the government has refused to intervene.

---

[128] *See, e.g.*, SUSAN W. BRENNER, CYBERTHREATS: THE EMERGING FAULT LINES OF THE NATION STATE 65-70 (2009) [hereinafter BRENNER, CYBERTHREATS]. Since the attacks target computers and servers located in the territory of another nation-state, they could be analogized to the Japanese bombing of Pearl Harbor or Hitler's invading Poland. *See id.*

[129] *Id.*

[130] *See, e.g.*, BRENNER, CYBERTHREATS, *supra* note 128, at 235-38; *see generally id.* at 105-09.

[131] For an analysis of the cyberwarfare issues, see *id.* at 65-70.

Since the attacks target civilian entities, the responsibility for responding to them lies with civilian law enforcement. We will assume the FBI takes the lead in dealing with this situation. We will also assume that the FBI decides the best way to respond to the "harm" being inflicted by the external site is to use DDoS attacks to shut the site down.

The legal issue we then need to address is whether using DDoS attacks to shut down an external website implicates the Fourth Amendment. It presumably does not: The Supreme Court has held that the Fourth Amendment protects "the people of the United States against arbitrary action by their own Government," but in no way "restrain[s] the Federal Government's actions against aliens outside United States territory."[132] And in *United States v. Gorshkov,* a federal judge held that FBI agents do not violate the Fourth Amendment by accessing a Russian computer and downloading data without being authorized to do so.[133]

We could end this analysis by deciding there is no need to address the Fourth Amendment implications of using DDoS attacks against an external website. That is probably what a court would do. However, I think it is useful to proceed by considering how the Fourth Amendment *could* apply to actions taken in the virtual world of cyberspace. I think such a consideration is a useful exercise because U.S. courts may well find it necessary to revise the interpretation that limits the applicability of the Fourth Amendment to extraterritorial actions, at least when those actions involve the use of cyberspace.[134]

---

[132] United States v. Verdugo-Urquidez, 494 U.S. 259, 260 (1990); *see supra* note 41 and accompanying text.

[133] *See supra* notes 107-08 and accompanying text. As noted earlier, the judge held that the FBI's actions were justified by the exigent circumstances exception to the Fourth Amendment's warrant requirement. United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001). He also held that the Fourth Amendment did not apply to the FBI agents' actions because the Russian computer was not in the United States and was not owned by a U.S. citizen. *See id.* at *3.

[134] Aside from other considerations, courts may decide to revise the rule because of the tensions it can cause with other countries. *See, e.g.*, Mike Brunker, *FBI Agent*

We will assume, for the purposes of analysis, that the Fourth Amendment *can* (but does not necessarily) apply to the use of DDoS attacks to shut down an external target that is inflicting "harm" on U.S. citizens.

For the Fourth Amendment to apply to such activity, it must involve a "search" or a "seizure." Since DDoS attacks do not involve accessing—hacking into—the target computers, it does not seem that our hypothesized retaliation would involve a search. That leaves a seizure as the only remaining option. In *U.S. v. Jacobsen*, the Supreme Court held that a seizure of property occurs when "there is some meaningful interference with an individual's possessory interest in that property."[135]

For the purposes of analysis, we will assume that the external website is "property" and is owned by an individual—Mr. X. For a U.S.-launched DDoS attack on the website to constitute a seizure, it would have to meaningfully interfere with Mr. X.'s possessory interest in that site. Since the value—the utility—of a website lies in its functionality, it is logical to assume that shutting down Mr. X's website would interfere with his possessory interest in that property.[136]

The next question is whether the seizure of the website would be reasonable.[137] To be reasonable, the seizure would have to be conducted pursuant to a warrant or to a valid exception to the warrant requirement.[138] If the FBI has time to obtain a warrant, this would be the preferable approach to ensuring that the seizure satisfies the requirements of the Fourth Amendment. If, as seems

---

Charged With Hacking, MSNBC (Aug. 15, 2002), http://www.msnbc.msn.com/id/3078784/ns/news-internet_underground/.

[135] 466 U.S. 109, 113 (1984) (footnote omitted).

[136] Federal courts have held, for example, that an officer's killing someone's dog constitutes a Fourth Amendment seizure. *See, e.g.*, Brown v. Muhlenberg, 269 F.3d 205, 210 (3d Cir. 2001). Since a DDoS attack does not permanently take a website offline, it would not constitute this type of absolute seizure, i.e., a complete deprivation of the property, but would constitute a meaningful "interference" with the property.

[137] *See, e.g.*, United States v. Ramirez, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis . . ." encompasses damage to property.).

[138] *See, e.g.*, Menotti v. City of Seattle, 409 F.3d 1113, 1154 (9th Cir. 2005). Warrants can authorize the use of force. *See, e.g.*, United States v. Husband, 226 F.3d 626, 639-40 (7th Cir. 2000).

more likely, the FBI decides it does not have time to get a warrant but must act quickly, then the agents could presumably rely on the exigent circumstances exception to the warrant requirement as justifying the DDoS attack.[139]

What might be involved in obtaining a DDoS warrant? The FBI agents would have to show they had probable cause to believe the seizure (the DDoS attack) was necessary to prevent and/or interrupt the commission of a federal crime and would have to particularly describe the target of the attack, i.e., Mr. X's website. They could no doubt use methods analogous to those described above, in the discussion of Trojan Horse warrants, to establish both. And, as with a Trojan Horse warrant, the DDoS warrant might also specify the time period for which the attack could be sustained and/or resumed if and when it was terminated or interrupted.[140]

The DDoS attacks might only be an interim measure—essentially, a cyber-*Terry* stop of a website. Since it would be difficult, if not impossible, to use DDoS attacks to take Mr. X's site permanently offline, the agents might want to resort to other types of cyber-force to accomplish that goal. They might, for example, want to use computer viruses or worms to destroy the site, which of course would require parsing the requirements for the use of those cyber-weapons and using the relevant Fourth Amendment principles to authorize their use.

CONCLUSION

When I finished the initial draft of this article in the early spring of 2011, the tactics analyzed above both were (at least as far as I knew) still mere possibilities. In April, 2011, the Department of Justice and the FBI launched a joint effort to take down a massive Coreflood botnet.[141]

---

[139] *See* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001).

[140] When the attack(s) finally ended, the agents could return it, together with a description of what was done to execute it, to the magistrate who issued it. *See* FED. R. CRIM. P. 41(f)(1)(D).

[141] As an FBI press release explained:

As part of that effort, the Department of Justice sought and obtained a temporary restraining order from a federal judge in Connecticut that let a nonprofit entity, working "under law enforcement supervision," seize and replace computer servers being used to operate the botnet with servers controlled by it and by the FBI.[142] The Justice Department's initial filing with the court also noted that this entity, again working "under law enforcement supervision," would "collect the IP addresses of all infected machines communicating with the criminal servers, and send a remote 'stop' command to infected machines to disable the Coreflood malware operating on them."[143]

In the Memorandum of Law the Department of Justice submitted in support of its request for the temporary restraining order, the Department argued that "stop[ping] the Coreflood virus" did not constitute either a search or a seizure under the Fourth Amendment.[144] According to the memorandum, there would be "no cognizable 'search' under the Fourth Amendment" because the government was not seeking authorization to "obtain or record any data that [was] on the infected computers."[145] It also argued that there was no seizure because the steps taken to stop the Coreflood infection would not "meaningfully interfere with a

---

> Botnets are networks of virus-infected computers controlled remotely by an attacker. They can be used to steal funds, hijack identities, and commit other crimes. The botnet in this case involves the . . . Coreflood virus, a key-logging program that allows cyber thieves to steal personal and financial information by recording unsuspecting users' every keystroke. Once a computer or network of computers is infected by Coreflood—infection may occur when users open a malicious e-mail attachment—thieves control the malware through remote servers.

Botnet Operation Disabled, FED. BUREAU OF INVESTIGATION (Apr. 14, 2011), http://www.fbi.gov/news/stories/2011/april/botnet_041411.

[142] Kim Zetter, *With Court Order, FBI Hijacks "Coreflood" Botnet, Sends Kill Signal*, WIRED (Apr. 13, 2011, 6:17 PM), http://www.wired.com/threatlevel/2011/04/coreflood/.

[143] *Id.*; *see supra* note 86 and accompanying text.

[144] *See* Government's Memorandum of Law in Support of Motion for Temporary Restraining Order, Preliminary Injunction, and Other Ancillary Relief at 46, United States v. John Doe, No. 3:11 CV 561 (VLB) (D. Conn. Apr. 12, 2011), *available at* http://www.steptoe.com/assets/attachments/4253.pdf.

[145] *Id.* at 46.

computer owner's possessory interests over an infected computer."[146]

As noted above, the Connecticut district court granted the temporary restraining order; eleven days later, the Department of Justice returned to the court, this time asking that the temporary restraining order "be continued as a preliminary injunction."[147] The memorandum submitted in support of this request asked that the authorization provided by the temporary restraining order be continued to allow the remediation efforts undertaken under the original order to continue; it noted that the efforts had significantly reduced the size of the Coreflood botnet, and should continue to do so if the authorization remained in effect.[148]

It also noted that the government intended to begin uninstalling Coreflood "from the computers of Identifiable Victims who provide written consent" to such measures.[149] In what was presumably an acknowledgment of the potential Fourth Amendment implications of such activity, the memorandum explained that the government was "not requesting explicit authorization from the Court" to initiate the uninstallation effort "because the written consent form obviates the need for such authorization."[150] As I write this, the court has not ruled on this request, but I will not be surprised if it is granted.

The U.S. government's 2011 initiative against the Coreflood botnet did not involve the use of Trojan Horse warrants, but I would argue that at least one aspect of it—the process of uninstalling the Coreflood virus from infected computers—involved the use of virtual force. The force was not directed at humans, but at a tool—or a weapon—cybercriminals were using to victimize U.S. citizens, among others. We can analogize "entering" the infected computers to eliminate the virus to scenarios in which law enforcement officers physically enter premises to disable an explosive device and/or disarm someone who is holding victims hostage. One scenario involves the use of physical force in a physical environment; the other involves the use of virtual force in a virtual environment. The scenarios obviously differ in certain empirical respects, but I, for one, would argue that the conduct at issue is functionally analogous, at least as far as the Fourth Amendment is concerned.

---

[146] *Id.* at 47. The memorandum also argued that eliminating the Coreflood virus from the computers did not constitute a seizure because the virus was an "instrumentality of crime," analogous to contraband. *Id.* at 51.

[147] Government's Supplemental Memorandum In Support of Preliminary Injunction at 15, United States v. John Doe, No. 3:11 CV 561 (VLB) (D. Conn. Apr. 23, 2011), *available at* http://www.justice.gov/opa/documents/coreflood-govt-supp.pdf.

[148] *Id.* at 9-15.

[149] *Id.* at 12.

[150] *Id.* at 12-13.

I may be wrong, but I suspect we will see more law enforcement activity moving into the virtual world. If I am correct in that suspicion, then we should see other uses of virtual force and the use of Trojan Horse warrants, along with other virtual analogues of the tactics law enforcement officers have traditionally used in the physical world.

THE FUTURE OF THE FOURTH AMENDMENT IN A DIGITAL EVIDENCE CONTEXT: WHERE WOULD THE SUPREME COURT DRAW THE ELECTRONIC LINE AT THE INTERNATIONAL BORDER?

Patrick E. Corbett[*]

INTRODUCTION 1264
I. *ABIDOR V. NAPOLITANO* AND BORDER SEARCHES OF ELECTRONIC STORAGE DEVICES 1266
II. VARIOUS LOWER COURT CASES 1269
  A. General Lessons 1270
  B. Transportation and Examination of Electronic Devices Beyond the Actual Border 1272
III. WHAT HAS THE U.S. SUPREME COURT HELD REGARDING BORDER SEARCHES? ANY GUIDANCE FROM NON-BORDER SEARCH CASES? 1277
  A. Border Search Cases 1277
  B. Non-Border Search Cases 1281
IV. OTHER RELEVANT CONSIDERATIONS 1285
  A. General Reflections on Justices of the Supreme Court 1285
  B. Perspectives of Justices in Various Oral Arguments 1287
    1. *United States v. Flores-Montano* 1288
    2. *City of Ontario, California v. Quon* 1290
  C. Potential Federal Legislation on Warrantless Border Searches of Electronic Devices 1293

---

[*] Professor of Criminal Law & Criminal Procedure, Thomas M. Cooley Law School, Lansing, Michigan. The author thanks the National Center for Justice and the Rule of Law, and Professor Thomas Clancy, for inviting him to participate in the 2011 Fourth Amendment Symposium. The author also wishes to acknowledge the detailed, timely, and academic research of Cooley Law School librarian, Jamie Baker, law students, Katherine Montgomery and Shawn Solon, as well as the helpful reflections of law student Jason Taylor.

D. Fourth Amendment and First Amendment Concerns at the Border 1297
E. Frequency of Border Searches of Electronic Storage Devices 1299
F. Impact of Encryption 1300
V. GENERAL REFLECTIONS 1304
CONCLUSION 1307

INTRODUCTION

In 1980, the United States Supreme Court stated that "[i]n terms that apply equally to seizures of property and to seizures of persons, the Fourth Amendment has drawn a *firm line at the entrance to the house*. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant."[1] In 2001, in ruling that law enforcement use of a thermal imager pointed at a home to gather information regarding heat within the home violated the Fourth Amendment, the Court revisited the "firm line": "That line, we think, must be not only firm but also bright—which requires clear specification of those methods of surveillance that require a warrant."[2]

The Court has certainly made clear that what goes on in the home is private and heavily protected by the Fourth Amendment. Are there other areas where one's expectation of privacy is so high that the Court should draw a similar line? What about the intimate details of one's personal life that can be stored on a laptop computer (or other electronic devices)? Should United States Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) agents be allowed to search these items at the international border without any individualized suspicion? If they seize them without any suspicion, how long can they hold them, and how extensively can they search them before they run afoul of the Fourth Amendment? If the United States Supreme Court is faced with these questions, how will it likely rule?

---

[1] Payton v. New York, 445 U.S. 573, 590 (1980) (emphasis added).

[2] Kyllo v. United States, 533 U.S. 27, 40 (2001).

In a day and age when everyone travels with electronic devices—such as cell phones, laptops, flash drives, and digital cameras—it should come as no surprise that these devices are subject to a search when entering the United States.[3] While some sort of individualized suspicion is typically necessary for a search of one's personal belongings to be constitutional under the Fourth Amendment, the border search has been a longstanding exception to that rule. As a general matter, the high government interest in national security has empowered the Court to allow most border searches to occur without any individualized suspicion. While the law on border searches seems rock solid, will the deeply personal and private nature of data stored on electronic devices empower a change in the law? Will the vastness of the storage capacity of these devices motivate the Court to re-examine Fourth Amendment principles at the international border?

Using a case involving an international border search of a laptop, this Article will explore the future of the Fourth Amendment in a digital evidence context. Section I will review *Abidor v. Napolitano*,[4] a case recently filed by the American Civil Liberties Union and other entities asserting that United States border patrol policies that allow full searches of electronic storage devices, like a laptop computer, without any individualized suspicion violate the Fourth Amendment.[5] Section II will summarize what other courts have ruled in similar contexts. Section III will briefly examine Supreme Court border search cases and other arguably applicable Supreme Court opinions. Section IV will consider an assortment of concepts in an attempt to examine how a future panel of the United States Supreme Court might rule if faced with the issues presented in *Abidor*. The Article will conclude with parting reflections on how a future panel of the Supreme Court might rule. Will the Court draw an electronic line similar to that "firm line" at the entrance to the home?

---

[3] Growing up near Detroit's Ambassador Bridge, linking Detroit to Windsor, Ontario, this author is no stranger to crossing the border and being extensively questioned or searched at the border. In fact, the Ambassador Bridge is North America's busiest border crossing. Detroit Int'l Bridge Co. v. Fed. Highway Admin., No. 09-13805, 2010 U.S. Dist. LEXIS 13671, at *1 n.1 (E.D. Mich. Feb. 17, 2010).

[4] Complaint, Abidor v. Napolitano, No. CV10-4059 (E.D.N.Y. filed Sept. 7, 2010) [hereinafter Abidor Complaint]. While the future of the *Abidor* case is unclear, the facts of *Abidor* provide a great backdrop for examination of the Fourth Amendment in the context of electronic devices at the border. This Article will not explore the likelihood that the *Abidor* case, or a similar case, will be accepted by the U.S. Supreme Court for review. For purposes of this Article, the author requests the reader to assume that the Court is willing to review such a case—how would they rule?

[5] Individuals seeking redress for losses due to the international border seizure and search of their laptops are not limiting themselves to Fourth Amendment claims. *See, e.g.*, Kam-Almaz v. United States, 96 Fed. Cl. 84 (Fed. Cl. 2011) (Due to jurisdictional concerns, plaintiff unsuccessfully sought redress under a breach of contract theory and the "takings" clause of the Fifth Amendment.).

I. *ABIDOR V. NAPOLITANO* AND BORDER SEARCHES OF ELECTRONIC STORAGE DEVICES

On September 7, 2010, Pascal Abidor, a Ph.D. student in Islamic studies studying in Canada with dual U.S. and French citizenship, and other plaintiffs,[6] filed a complaint against Secretary of the Department of Homeland Security (DHS), Janet

---

[6] Pascal Abidor is joined in this lawsuit by the National Association of Criminal Defense Lawyers (NACDL) and the National Press Photographers Association (NPPA). This case study will primarily focus on the situation faced by Pascal Abidor.

Plaintiff NACDL is a non-profit organization of criminal defense lawyers with a particular interest on the impact modern national security policies have had on First, Fourth, Fifth, and Sixth Amendment rights. Abidor Complaint, *supra* note 4, at 16. According to the complaint, in the course of their work, many NACDL attorneys often travel abroad to represent their clients and bring along electronic devices to record their work product, which necessarily contain confidential client information protected by the attorney-client privilege. *Id.* at 16-24. In today's society, NACDL asserts it is nearly impossible for attorneys to perform their duties without the aid of electronic devices, such as laptops. *Id.* According to the complaint, at least one member of the NACDL, criminal defense attorney Lisa M. Wayne, had her laptop searched during a forty-five minute long detention upon entering the United States after a business trip to Mexico. *Id.* 21-22.

Plaintiff NPPA is composed of 7000 professional and freelance photojournalists who advocate the free dissemination of information and images around the world. *Id.* at 25. According to the complaint, many of their members frequently travel the world to cover news stories including foreign conflicts of interest to the United States government. *Id.* at 26-27. They record their findings via text, images, video, audio recordings, and the like on various forms of electronic devices such as laptops. They assert that the Department of Homeland Security regulations put their First Amendment-protected and confidential material at risk of exposure when crossing the border, and detention of their devices makes it impossible for them to meet deadlines. *Id.* at 31-33. According to the complaint, NPPA member Duane Kerzic, a freelance photographer, had his laptop searched during his trip back from Canada to take photographs of lighthouses and national parks. *Id.*

Napolitano, attacking two new CBP and ICE policies of DHS[7] issued in August 2009.[8] In the complaint, Abidor asserted that the United States border patrol policies that allow full searches of electronic storage devices, like a laptop computer, without any individualized suspicion, violate the violate the First and Fourth Amendments.[9]

In May 2010, Pascal Abidor was traveling via Amtrak train from Montreal, Canada to New York City.[10] Abidor had recently traveled to Jordan and Lebanon for academic purposes.[11] When the train arrived at the CBP point at the Canada–United States border, routine questioning of Abidor led the CBP officer to request that Abidor sign into his password-protected laptop for an additional search of the electronic data it contained.[12] The CBP officer perused some of his personal data (such as photos and saved chat conversation with his girlfriend) and some information and images downloaded for research purposes, including images of Hamas and Hezbollah rallies.[13] After writing down the password for the officer, Abidor was frisked and then transferred to Service Port-Champlain where he was detained in a small cinderblock cell and questioned for several hours.[14] After he was released, officers retained his laptop and external hard drive.[15] He was given a "Detention Notice and Custody Receipt for Detained Property" that indicated the devices were being held by ICE.[16] The devices were returned eleven days later after Abidor's attorney contacted authorities on his behalf.[17] Abidor examined his laptop after it was returned and concluded that "the casing and warranty seal [had been] broken open" and that "officers from ICE, CBP and/or other agencies had examined basic directory folders on his laptop such as 'library' and 'users,' as well as backup documents that he had stored on his external hard drive."[18] According to Abidor's complaint, Abidor continues to cross the border for academic purposes and is repeatedly questioned about this incident.[19]

---

[7] U.S. CUSTOMS AND BORDER PROTECTION, BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION, CBP DIRECTIVE NO. 3340-049 (2009) [hereinafter 2009 CBP DIRECTIVE], *available at* http://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf; U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, BORDER SEARCHES OF ELECTRONIC DEVICES, ICE DIRECTIVE NO. 97-6.1 (2009) [hereinafter 2009 ICE DIRECTIVE], *available at* http://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf. CBP and ICE are two components of the United States Department of Homeland Security. *See* DEPARTMENT OF HOMELAND SECURITY, http://www.dhs.gov/index.shtm (last visited Jan. 25, 2012).

[8] *See* Abidor Complaint, *supra* note 4, at 4.

[9] *See id.* at 25-33. At the time of this writing, the *Abidor* complaint was still pending in the United States District Court for the Eastern District of New York. For a status update, see the U.S. District Court Civil Docket for the *Abidor* case at: http://dockets.justia.com/docket/new-york/nyedce/1:2010cv04059/308557/.

[10] *See* Abidor Complaint, *supra* not 4, at 8.

[11] *Id.*

[12] According to Abidor, the CBP officer "*ordered* Mr. Abidor to enter his password. Mr. Abidor *complied* with the order." *Id.* at 9 (emphasis added).

[13] *Id.*

[14] *See id.* at 9-10. According to Abidor, the "officers *ordered* Mr. Abidor to write down his password. Mr. Abidor *complied* with this order." *Id.* at 9 (emphasis added). In contrast, the U.S. Department of Justice asserts, "The CBP officers *asked* Abidor to write down the password for his laptop . . . ." Def's Mem. of Law in Supp. of Mot. to

In his complaint, Abidor asserts that current CBP and ICE policies violate the Fourth Amendment (and First Amendment) because they allow "suspicionless search, copying, and detention of electronic devices containing expressive, protected materials."[20] Furthermore, present policies authorize the search even if the owner of the device is not present.[21] Additionally, the policies "permit border officials, without any suspicion of wrongdoing, to detain a traveler's electronic devices, or copies of the contents thereof, for the purpose of further reading and analysis even after the traveler has left the border."[22] Under certain circumstances, CBP and ICE may share this information "with other government agencies or third parties even where there is no suspicion of wrongdoing."[23]

Dismiss at 9, Abidor v. Napolitano, No. CV10-4059 (E.D.N.Y. Jan. 28, 2011) (emphasis added).

[15] *See* Abidor Complaint, *supra* note 4, at 11.

[16] *Id.*

[17] *See id.* at 12.

[18] *Id.*

[19] *See id.* at 13-14. This Article will not explore whether Pascal Abidor, or the other plaintiffs, have standing to obtain the declaratory and injunctive relief that they seek. While standing is clearly an issue in the United States District Court, this Article will assume, *arguendo*, that the plaintiffs have standing, and will only explore the merits of the Fourth Amendment concerns.

[20] *Id.* at 33.

[21] *See id.* at 5.

[22] *Id.*

[23] *Id.*

While it is unclear what direction this case will go, the problem is apparent: International border searches of electronic devices have the potential to seriously impact the personal and professional privacy of individuals. In granting a motion to suppress child pornography obtained from a laptop during a suspicionless search at the border, the U.S. District Court in *United States v. Arnold*[24] stated the concern well:

> Fourth Amendment protection extends to the search of this type of personal and private information at the border. While not physically intrusive as in the case of a strip or body cavity search, the search of one's private and valuable personal information stored on a hard drive or other electronic storage device can be just as much, if not more, of an intrusion into the dignity and privacy interests of a person. This is because electronic storage devices function as an extension of our own memory. They are capable of storing our thoughts, ranging from the most whimsical to the most profound. Therefore, government intrusions into the mind—specifically those that would cause fear or apprehension in a reasonable person—are no less deserving of Fourth Amendment scrutiny than intrusions that are physical in nature.[25]

II. VARIOUS LOWER COURT CASES

Lower courts have had the opportunity in the recent past to consider the constitutionality of the border search exception in the context of electronic devices. This Section will briefly discuss some important lessons obtained from a review of various lower court cases.[26]

---

[24] 454 F. Supp. 2d 999, 1003 (C.D. Cal. 2006) (holding that officers needed reasonable suspicion to search the laptop and that, since reasonable suspicion was not present, the search violated the Fourth Amendment).

[25] *Id.* at 1000-01. The U.S. Court of Appeals for the Ninth Circuit reversed, holding that, based on a review of the U.S. Supreme Court border search cases, "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border." United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008), *cert. denied*, 129 S. Ct. 1312 (2009).

[26] The following cases were examined: *United States v. Cotterman*, 637 F.3d 1068 (9th Cir. 2011); *United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008); *United States v. Irving*, 452 F.3d 110 (2d Cir. 2006); *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005); *United States v. Hanson*, No. CR 09-00946 JSW, 2010 WL 2231796 (N.D. Cal. June 2,

A. General Lessons

All of the cases reviewed involve crimes pertaining to child sexual abuse or child pornography. One researching international border searches of electronic devices will find that the large majority of cases involve child pornography—it is the rare case that involves *any* crime other than child pornography.[27] Not surprisingly, possibly due to the presence of the child pornography, none of the cases reviewed ultimately suppressed the evidence that was found in the assorted electronic devices.

Child pornography is not involved in the case of Pascal Abidor. Abidor is an academic and his data relates to Islamic studies.[28] Breaking from the category of child pornography, it is reasonable to think of many other kinds of data that could theoretically be located on an electronic device at the border: protected trade secrets, material to be published, attorney-client privileged material, and deeply personal information like tax returns and banking information. Should the fact that Abidor's case does not involve child pornography mean it should be treated differently at the border? At a minimum, it might invite greater scrutiny by a court.

Many of the cases discussed "routine" versus "non-routine" border searches, noting that "routine" searches do not require any suspicion while "non-routine" searches generally require some kind of individualized suspicion. Most of the cases, however, avoided this question, simply finding that reasonable suspicion

---

2010) (designated "not for citation"); *United States v. Stewart*, 715 F. Supp. 2d 750 (E.D. Mich. 2010); *United States v. Rogozin*, No. 09-CR-379(S)(M), 2010 U.S. Dist. LEXIS 121162 (W.D.N.Y. Nov. 16, 2010); *Cancel-Ríos v. United States*, No. 10-1386, 2010 U.S. Dist. LEXIS 90336 (D.P.R. Aug. 30, 2010); *United States v. Bunty*, 617 F. Supp. 2d 359 (E.D. Pa. 2008); *United States v. Verma*, No. H-08-699-1, 2010 U.S. Dist. LEXIS 34559 (S.D. Tex. Apr. 8, 2010); *United States v. Pickett*, No. 07-0374, 2008 WL 4330247 (E.D. La. Sept. 16, 2008); *United States v. McAuley*, 563 F. Supp. 2d 672 (W.D. Tex. 2008), *aff'd*, No. 10-50470, 2011 U.S. App. LEXIS 6801 (5th Cir. Mar. 31, 2011); *United States v. Hampe*, No. 07-3-BW, 2007 WL 1192365 (D. Me. Apr. 18, 2007), *aff'd*, 2007 WL 1806671 (D. Me. June 19, 2007); and *United States v. Furukawa*, No. 06-145, 2006 U.S. Dist. LEXIS 83767 (D. Minn. Nov. 16, 2006).

[27] *See, e.g.*, United States v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007) (stating that in context of ecstasy-importation scheme, searches of "[d]ata storage media and electronic equipment" are included in routine border searches without any suspicion).

[28] *See* Abidor Complaint, *supra* note 4, at 8.

existed under the facts.[29] In at least one case, in denying the motion to suppress the child pornography images found by CBP agents in various electronic storage devices, the court held that even though reasonable suspicion was present justifying the search, reasonable suspicion was not necessary.[30] Some of the courts simply held that searching electronic devices is routine and requires no suspicion.[31] Finally, while not ruling for the defendant, some courts have considered whether First Amendment considerations should impact on Fourth Amendment reasonableness analysis.[32]

---

[29] *See, e.g.*, United States v. Irving, 452 F.3d 110, 123-24 (2d Cir. 2006) (noting that "routine" searches of "a person's luggage or personal belongings" do not require any individualized suspicion and that a "border search is valid under the Fourth Amendment, even if non-routine, if it is supported by reasonable suspicion," and affirming the district court's decision to deny the motion to suppress the child sexually explicit material found on diskettes in the luggage because the search was supported by reasonable suspicion); United States v. Rogozin, No. 09-CR-379(S)(M), 2010 U.S. Dist. LEXIS 121162, at *9 (W.D.N.Y. Nov. 16, 2010) (The U.S. Magistrate Judge chose not to make a finding regarding whether the search was routine, and instead found under the facts that reasonable suspicion existed "which would justify examining the laptop during the secondary inspection."); United States v. Verma, No. H-08-699-1, 2010 U.S. Dist. LEXIS 34559, at *12 (S.D. Tex. Apr. 8, 2010) (noting that even if deemed "non-routine," facts supported presence of reasonable suspicion); United States v. Hampe, No. 07-3-BW, 2007 WL 1192365, at *4 (D. Me. 2007), *aff'd*, 2007 WL 1806671 (D. Me. 2007) (holding that search of laptop was routine search requiring no suspicion but even if it was deemed non-routine reasonable suspicion was present); United States v. Furukawa, No. 06-145, 2006 U.S. Dist. LEXIS 83767 (D. Minn. Nov. 16, 2006) (adopting the recommendation of the U.S. Magistrate Judge, but not concluding whether a search of electronic devices is routine or not; instead, the court simply stated reasonable suspicion for the search was present, so the motion to suppress was properly denied).

[30] *See* United States v. Bunty, 617 F. Supp. 2d 359, 365 (E.D. Pa. 2008) ("Defendant has not pointed to any aspect of the . . . border search that would distinguish it from other routine computer searches at the border.").

[31] *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1008 n.2 (9th Cir. 2008) (holding that, based on a review of the United States Supreme Court border search cases, "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border"); Cancel-Ríos v. United States, No. 10-1386, 2010 U.S. Dist. LEXIS 90336, at *9 (D.P.R. Aug. 30, 2010) (denying habeas corpus petition and holding that Cancel-Ríos could not have prevailed on a motion to suppress evidence of child pornography found by CBP agents on a cell phone and had effective assistance of counsel because "[i]n the context of a border search, a warrantless, suspicionless search of property ordinarily will not run afoul of the owner's Fourth Amendment rights"); United States v. Verma, No. H-08-699-1, 2010 U.S. Dist. LEXIS 34559, at *11 (S.D. Tex. Apr. 8, 2010) (denying the motion to suppress child pornography images taken from a CD by ICE agents and holding that the search did not need any individualized suspicion because it was "routine"; a search is routine as long as it did not "invade Verma's body or damage his computer"); United States v. McAuley, 563 F. Supp. 2d 672, 678 (W.D. Tex. 2008) (holding laptops are not "per se embarrassing" and are part of a routine border search, meaning reasonable

Can the court jump right to reasonable suspicion with *Abidor*? Assuming the facts alleged in the complaint are accurate, the agents might have a "hunch" regarding criminal activity, but seemingly no reasonable suspicion of criminal activity. He did not appear nervous, was very cooperative, and only had images of Hamas and Hezbollah rallies. If reasonable suspicion was not present, was the conduct of the agents in the initial seizure and search of the laptop, as well as any later searches, constitutional? Should the agents' conduct be subjected to greater scrutiny given the First Amendment implications?

B. Transportation and Examination of Electronic Devices Beyond the Actual Border

Some courts have voiced concern with the length of time agents possessed the electronic devices after the initial seizure at the border. In *United States v. Stewart*, agents randomly chose Stewart for questioning upon his return flight from Asia.[33] His uncooperative behavior led to a secondary search of his belongings, including two laptops, a digital camera, and three computer memory sticks.[34] Although the camera and memory sticks contained no contraband, the first laptop contained approximately a dozen photographs depicting child pornography.[35] The second laptop had a dead battery and authorities determined that they did not have the means to search it at the airport—

---

suspicion is not required), *aff'd*, No. 10-50470, 2011 U.S. App. LEXIS 6801 (5th Cir. Mar. 31, 2011) (holding that because McAuley voluntarily consented to the search, there was no need to evaluate border search question).

[32] *See* United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005) ("Particularly in today's world, national security interests may require uncovering terrorist communications, which are inherently 'expressive.'") (noting that there has never been a First Amendment exception to the warrant requirement and, therefore, no First Amendment exception to border search); *Arnold*, 533 F.3d at 1010 (dismissing summarily Arnold's First Amendment argument and stating that "despite Arnold's arguments to the contrary we are unpersuaded that we should create a split with the Fourth Circuit's decision in *Ickes*").

[33] 715 F. Supp. 2d 750 (E.D. Mich. 2010).

[34] *Id.* at 751

[35] *Id.*

requiring them to send both laptops to ICE headquarters about twenty miles away for a forensic search the following day.[36]

Stewart did not contend that the initial search of the laptops violated the Fourth Amendment, but rather argued that the evidence obtained from them should be suppressed because the continued retention of the computers and transport to a distant location was unreasonable.[37] The court agreed that this action by authorities was more invasive than a routine border search, but stated there was no Fourth Amendment violation because there was reasonable suspicion that the computer contained contraband based upon the images found on the first laptop during the initial search.[38] This reasonable suspicion rendered the further detention and transport of the computer constitutional.[39]

In *United States v. Rogozin*, Rogozin, a German citizen with lawful permanent residency in New York, was returning to New York from Canada.[40] He indicated to agents that he had visited Niagara Falls overnight as a tourist.[41] The CBP officer found his demeanor to be suspicious because his responses were hesitant, he did not maintain eye contact, and he had traveled all the way from Brooklyn for a one day stay in Canada.[42] The secondary inspection of Rogozin's laptop, camera, iPhone, and video recorder revealed photographs of small children in "sexually suggestive positions."[43] ICE agents then arrived to do a more extensive search of the electronic devices. In reviewing the laptop, the ICE agents "saw some images of naked children, and others in provocative poses."[44]

---

[36] *See id.* at 751-52.

[37] *See id.* at 753. Stewart contended that seizing the computer at the border and then transporting it to another location was "the equivalent of an extended border search that required justification by some level of government suspicion, which was not present in this case." *Id.* at 752. Courts that have utilized the concept of "extended border searches" have generally held that searches that are "removed in time and place from the actual border" are justified by reasonable suspicion that the subject of the search was involved in some kind of criminal conduct. *Id.* at 754 (citing United States v. Guzman-Padilla, 573 F.3d 865, 877-78 (9th Cir. 2009); United States v. Niver, 689 F.2d 520, 526 (5th Cir. 1982)).

[38] *See id.* at 754-55.

[39] *Id.*

[40] No. 09-CR-379(S)(M), 2010 U.S. Dist. LEXIS 121162 (W.D.N.Y. Nov. 16, 2010).

[41] *See id.* at *2.

[42] *Id.* at *3.

[43] *Id.*

[44] *Id.* at *5.

In an interview, Rogozin told the agents that he had seen child pornography on his computer.[45]

The agents decided to retain the laptop and other devices for a forensic examination, and Rogozin was allowed to enter the United States.[46] Four days later, ICE agents conducted a forensic examination of the laptop and discovered 185 photographs of "pretty obvious" child pornography.[47] The agents subsequently obtained a search warrant for the laptop but not for the camera, video recorder or iPhone.[48] Agents arrested Rogozin in his home in Brooklyn approximately two and a half months after the border stop.[49] It appears from the case that none of the electronic devices were returned during the two and a half month period.

The court noted that it "need not decide whether or not the search of the laptop computer can be considered 'routine'" because Rogozin's demeanor at the initial interview, including failure to maintain eye contact, created reasonable suspicion to search the computer.[50] According to the court, the initial discovery of the suggestive photos justified the more detailed search four days later and "[t]he four-day delay between the initial inspection . . . and the follow-up inspection . . . does not invalidate the search."[51] As the results of the second search properly led to probable cause for the warrant for the laptop, the court denied the motion to suppress the evidence obtained from the laptop.

On the other hand, the court did suppress the evidence obtained from the video recorder, iPhone, and camera. Noting that the initial search did not reveal child pornography, the court stated that the "government offers no legitimate excuse [for] continuing to hold the video recorder for this length of time without seeking a warrant."[52] While the initial border search of these items did demonstrate sexually suggestive photographs of children, none of the photographs found were truly pornographic and, therefore, not illegal. Thus, the judge found that the continued seizure of these items was inappropriate, and thus any evidence from the video recorder, I-phone, and camera was inadmissible.[53]

---

[45] *Id.*

[46] *Id.* at *6.

[47] *Id.* at *3.

[48] Is it significant that the agents, sua sponte, chose to obtain a search warrant? If they did not need to, why did they? Does it indicate that they were merely acting cautiously? Or might it indicate that the agents were acting to avoid a violation of the Constitution in holding the laptop too long? In other cases, agents acted similarly in obtaining a warrant. *See, e.g.*, United States v. Pickett, No. 07-0374, 2008 WL 4330247 (E.D. La. Sept. 16, 2008) (agents could not easily view images on the laptop, thus, they obtained a search warrant to do a more detailed search).

[49] *See Rogozin*, 2010 U.S. Dist. LEXIS 121162, at *3.

[50] *Id.* at *9.

[51] *Id.* at *9-10.

In *United States v. Cotterman*, the Ninth Circuit held that a search of a laptop that lasted two days and encompassed 170 miles was nevertheless protected by the border search exception to the Fourth Amendment.[54] This reversed the district court's decision, which had ruled to exclude hundreds of pornographic images of children found on the defendant's laptop, including photos of the defendant molesting children.[55]

Cotterman's past criminal convictions for sexual crimes against children prompted customs officials to perform a secondary search when he crossed the Mexican border into Lukeville, Arizona.[56] Officers found two laptops and three digital cameras in his vehicle, but the files were password-protected.[57] Officers transferred the devices to Tucson, and two days later, the illegal images were located.[58]

Cotterman did not dispute the validity of the border search exception or its application to the initial search at the border, but argued that the search in Tucson required reasonable suspicion. The court characterized the issue and its holding as follows: "The sticking point is whether the inherent power of the Government to subject incoming travelers to inspection before entry also permits the Government to transport property not yet cleared for entry away from the border to complete its search. Cotterman claims that it does not. We cannot agree."[59] Despite the physical distance and lapse of time, the court held that this was one continuous search, beginning at the border. Noting that the "border search doctrine is guided—like all Fourth Amendment jurisprudence—by reason and practicality, not inflexible rules of time and space,"[60] the court held that no individualized suspicion is necessary and that "[s]o long as property has not been officially cleared for entry into the United States and remains in the control of the Government, any further search is simply a continuation of the original border search—the entirety of which is justified by the Government's border search power."[61] Further noting, however, that these types of searches need to be analyzed on a "case-by-case basis to determine whether the scope or duration of the intrusion was constitutionally unreasonable,"[62] the court was careful to emphasize that in effectuating the border search the government does not have "carte blanche at the border to do as it pleases absent any regard for the Fourth Amendment."[63]

---

[52] *Id.* at *11. As for the camera and iPhone, the court noted that the record does not clearly indicate whether they are "still in the government's possession." *Id.* at *11 n.6.

[53] *See id.* at *12. Similarly, in *United States v. Hanson*, the court held that holding a laptop for five months after the initial border seizure in order to do a more detailed forensic examination required a search warrant. No. CR 09-00946 JSW, 2010 WL 2231796 (N.D. Cal. June 2, 2010) (designated "not for citation").

[54] 637 F.3d 1068 (9th Cir. 2011).

[55] *Id.* at 1070.

[56] *Id.* at 1071.

[57] *Id.*

[58] *See id.* at 1072.

The initial search of Abidor's laptop merely demonstrated his research material on Islam and jihadists, which can be legally possessed. The images of Hezbollah rallies are no worse than the sexually suggestive images of children that did not technically constitute child pornography found on Rogozin's video recorder, iPhone, and camera. Should the laptop have been immediately returned to Abidor?

Abidor has a stronger argument than both Stewart and Cotterman regarding the transport and detention of both himself and his electronic devices. Abidor and his belongings were transported from the train station to Service-Port Champlain for further questioning, which the complaint states is "far-away" from the Amtrak station.[64] After several hours of questioning in a small cell and Abidor's subsequent release, Abidor's laptop was then held for an additional eleven days. This is seemingly much more intrusive than the detention of Stewart's and Cotterman's electronic devices. The *Stewart* court mentioned that Stewart could have made the argument that the detention of his laptops was in essence a "full blown seizure requiring probable cause."[65] Should the court entertain the argument that the detention of his electronic devices was such a "full-blown seizure" that the agents needed reasonable suspicion or even probable cause to continue to hold those devices? Using the "case-by-case" basis referenced in *Cotterman*, is the *Abidor* case the one where the Supreme Court will draw the line on reasonableness?

---

[59] *Id.* at 1076.

[60] *Id.*

[61] *Id.* at 1079. Based upon language provided by the United States Supreme Court in past cases, the court listed three instances in which reasonable suspicion may be necessary for searches at the border: (1) highly intrusive searches of the person, (2) highly destructive searches of property, and (3) particularly offensive searches. According to the court, Cotterman's search did not fit into any of the categories. *Id.* at 1079-82.

[62] *Id.* at 1083.

[63] *Id.* at 1079.

[64] Abidor Complaint, *supra* note 4, at 15.

III. WHAT HAS THE U.S. SUPREME COURT HELD REGARDING BORDER SEARCHES? ANY GUIDANCE FROM NON-BORDER SEARCH CASES?

A. Border Search Cases

As the Ninth Circuit in *Cotterman* aptly noted: "We need not dwell long on the general scope of the Government's border search power. It is well-established that the sovereign need not make any special showing to justify its search of persons and property at the international border."[66] Much has been written about the Supreme Court cases discussing searches at the border,[67] so this Section will only highlight a few key points from those cases.

As a general matter, no suspicion is necessary to do a typical search of a person or property at the border. As the Court stated over thirty years ago in *United States v. Ramsey*,[68] in the context of a customs inspection of mail:

> [S]earches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this

---

[65] United States v. Stewart, 715 F. Supp. 2d 750, 755 (E.D. Mich. 2010).

[66] *Cotterman*, 637 F.3d at 1074 (citing United States v. Flores-Montano, 541 U.S. 149, 152-53 (2004)).

[67] *See, e.g.*, Symposium, *The Fourth Amendment at the International Border*, 78 MISS. L.J. i, i-430 (2008); *Warrantless Searches and Seizures*, 39 GEO. L.J. ANN. REV. CRIM. PROC. 43, 117-23 (2010).

[68] 431 U.S. 606 (1977).

> country, are reasonable simply by virtue of the fact that they occur at the border. . . . Border searches, then, from before the adoption of the Fourth Amendment, have been considered to be "reasonable" by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause. This longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless "reasonable" has a history as old as the Fourth Amendment itself.[69]

In *United States v. Montoya de Hernandez*,[70] Customs agents "reasonably suspect[ed] that the traveler [was] smuggling contraband in her alimentary canal."[71] The agents held her for sixteen hours until she expelled eighty-eight balloons of cocaine.[72] Recognizing that this is not a routine matter at the border, the Court indicated that the detention was appropriate because the "facts, and their rational inferences, known to [the] customs inspectors . . . clearly supported a reasonable suspicion that respondent was an alimentary canal smuggler."[73] Given the substantial national interest in preventing drugs from entering the country, the Court held "that the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal."[74]

Does *Montoya de Hernandez* have some direct application to Abidor's situation?[75] Is holding a person for sixteen hours to wait for a bowel movement the equivalent of holding a person for several hours in a small cinder block cell, requiring that person to provide the password so that agents can look at the laptop, then holding that laptop for eleven days? Abidor may argue that, when examined as a whole, the conduct of the CBP agents was particularly intrusive and should require reasonable suspicion (and that the CBP agents did not have reasonable suspicion). Abidor could argue that the detaining of a computer for eleven days and searching that computer is no different than holding a person for sixteen hours while waiting for a bowel movement.

---

[69] *Id.* at 616, 619.

[70] 473 U.S. 531 (1985).

[71] *Id.* at 541.

[72] *Id.* at 532-33.

[73] *Id.* at 542.

[74] *Id.* at 541.

[75] *See* Jennifer M. Chacon, *Border Searches of Electronic Data,* LexisNexis Expert Commentary, 2008 EMERGING ISSUES 2430 (June 2008) ("In *United States v. Montoya de Hernandez*, the Court found that the search of a traveler's 'alimentary canal,' achieved by detaining the traveler for sixteen hours until she passed the drugs that she had ingested, could not be conducted in the absence of individualized suspicion.

The *Montoya de Hernandez* Court goes on to state: "It is also important to note what we do *not* hold. Because the issues are not presented today, we suggest no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches."[76] The Court's usage of the phrase "such as" suggests that the "nonroutine" border searches are not limited to strip, body cavity, or x-ray searches—they could decide to include the search of electronic devices like a laptop.[77]

The Court in *Montoya de Hernandez*, however, did not specifically indicate that any level of suspicion was required for more intrusive searches of a person. In *United States v. Flores-Montano*, the Court intimates that some level of suspicion would be required.[78] In *Flores-Montano*, a person with a 1987 Ford Taurus wagon wanted to enter California from Mexico.[79] After referral to secondary inspection, a mechanic under contract with the government disassembled the gas tank within one hour and found thirty-seven kilograms of marijuana.[80] The Court upheld the suspicionless search of the gas tank, noting: "But the reasons that might support a requirement of some level of suspicion in the

---

Instead, the Court found that the dignity and privacy interests at stake required that such searches be conducted only where government officials had 'reasonable suspicion' of criminal activity.... This is the legal context in which border laptop searches have unfolded.").

[76] *Montoya de Hernandez*, 473 U.S. at 541 n.4.

[77] In *United States v. Flores-Montano*, the Court rejected the idea of creating a balancing test based on the "routine" and "nonroutine" framework, indicating that these are only "descriptive term[s] in discussing border searches." 541 U.S. 149, 152 (2004).

[78] *Id.*

[79] *Id.* at 150.

[80] *Id.* at 150-51.

case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles."[81]

Abidor will likely argue that the search of his laptop is more like the "highly intrusive searches of the person" and not like the gas tank search in *Flores-Montano*. As such, it is entitled to greater protection and requires, at a minimum, reasonable suspicion. The government will likely respond by arguing that a search of a computer, a piece of property outside of the body, cannot be compared to a highly intrusive search of the person. *Flores-Montano* has already set the precedent that a highly intrusive search of a vehicle's gas tank, a mere piece of property, does not require individualized suspicion.

The *Flores-Montano* Court goes on to make some open-ended statements that have surfaced in lower court cases discussing searches of electronic devices at the border.[82] Regarding border searches conducted in a "particularly offensive manner," the Court states: "We again leave open the question 'whether, and under what circumstances, a border search might be deemed "unreasonable" because of the particularly offensive manner it is carried out.'"[83] As for "destructive" searches, the Court notes: "While it may be true that some searches of property are so destructive as to require a different result, this was not one of them."[84]

Abidor may be able to fit the search of his laptop into one of these two narrow exceptions.[85] In *Arnold* and *Cotterman*, the Ninth Circuit rejected such an attempt in the context of laptops.[86] Both cases, however, involved child pornography and clear evidence that crime was discovered right at the border or within two days of the initial border stop. In the *Abidor* case, in contrast, the crime, if any, was some kind of terrorist-related activity, and no evidence of such crime was uncovered at the border or during the eleven days that Abidor's computer was held. Even if Abidor concedes that his laptop is property (and not analogous to a highly intrusive search of a person) and that the search of his laptop was not destructive, was the search carried out in a particularly offensive manner? Is the *Abidor* case the kind of situation envisioned by the Ninth Circuit when they implied that a search of a laptop could be "constitutionally unreasonable" based upon "the scope or duration of the intrusion"?[87] Might the Supreme Court agree?

---

[81] *Id.* at 152.

[82] *See, e.g.*, United States v. Cotterman, 637 F.3d 1068, 1079-82 (9th Cir. 2011); United States v. Arnold, 533 F.3d 1003, 1007-11 (9th Cir. 2008).

[83] United States v. Flores-Montano, 541 U.S. 149, 154-55 n.2 (citing United States v. Ramsey, 431 U.S. 606, 618 n. 13 (1977)).

[84] *Id.* at 155-56.

[85] *See* Erick Lucadamo, *Reading Your Mind at the Border: Searching Memorialized Thoughts and Memories on Your Laptop and United States v. Arnold*, 54 VILL. L. REV. 541, 572 (2009) ("[I]n the border search context, courts should analyze a laptop as an object, subject only to the two exceptions laid out by the *Flores-Montano* Court, i.e., those searches that are destructive of and particularly offensive to property.").

[86] *Cotterman*, 637 F.3d at 1079-82; *Arnold*, 533 F.3d at 1007-10.

B. Non-Border Search Cases

In *United States v. Martinez-Fuerte*, a decision concerning the use of vehicle checkpoints near the Mexican border, the Court provides some further guidance on concerns applicable in a border search context.[88] In *Martinez-Fuerte*, the Court did not interpret the border search exception. Instead, the Court analyzed the checkpoint under its government interest versus degree of intrusiveness (reasonableness) balancing test frequently used to interpret "special needs" types of searches. In affirming the use of the checkpoint utilized for the purpose of detecting illegal aliens, the Court noted:

> A requirement that stops on major routes inland always be based on reasonable suspicion would be impractical because the flow of traffic tends to be too heavy to allow the particularized study of a given car that would enable it to be identified as a possible carrier of illegal aliens. In particular, such a requirement would largely eliminate any deterrent to the conduct of well-disguised smuggling operations, even though smugglers are known to use these highways regularly.[89]

Is the *Martinez-Fuerte* language relevant to Abidor's case and the search of laptops at the border? The "traffic" and "deterrent" concerns are also applicable at the border.[90] *Martinez-Fuerte* does not extend much protection to Abidor because it suggests that the sheer volume of traffic at a border makes any requirement of reasonable suspicion wholly impractical. Moreover, the Court's concern about the impact that a reasonable suspicion requirement would have on any deterrent effect suggests the Court is disinclined to eliminate or restrict investigative techniques that might have a meaningful deterrent effect on crime.

---

[87] *Cotterman*, 637 F.3d at 1083.

[88] 428 U.S. 543 (1976).

[89] *Id.* at 557.

United States v. Place[91] also provides some guidance. In *Place*, Miami federal agents called New York federal agents and relayed information establishing reasonable suspicion that Place was flying into New York with illegal drugs on a Friday afternoon.[92] The New York agents stopped Place upon arrival at the airport and seized his luggage but allowed him to go on his way.[93] They then took the luggage to another airport across town for a dog sniff, which was positive as to one of the bags of luggage.[94] It took approximately ninety minutes from the initial seizure of the bag until the dog sniff.[95] Due to the late hour on Friday, officers held the bags until Monday when a warrant was obtained for the luggage. The agents found cocaine during the execution of the warrant.[96]

---

[90] *See* David Shipler, *Can You Frisk a Hard Drive?*, N.Y. TIMES, Feb. 19, 2011,at WK5, *available at* http://www.nytimes.com/2011/02/20/weekinreview/20laptop.html?_r=1 ("If you stand with the Customs and Border Protection officers who staff the passport booths at Dulles airport near the nation's capital, their task seems daunting. As a huge crowd of weary travelers shuffle along in serpentine lines, inspectors make quick decisions by asking a few questions (often across language barriers) and watching computer displays that don't go much beyond name, date of birth and codes for a previous customs problem or an outstanding arrest warrant. The officers are supposed to pick out the possible smugglers, terrorists or child pornographers and send them to secondary screening. The chosen few—6.1 million of the 293 million who entered the United States in the year ending Sept. 30, 2010—get a big letter written on their declaration forms: A for an agriculture check on foodstuffs, B for an immigration issue, and C for a luggage inspection. Into the computer the passport officers type the reasons for the selection, a heads-up to their colleagues in the back room, where more thorough databases are accessible.").

[91] 462 U.S. 696 (1983).

[92] *Id.* at 698.

[93] *Id.* at 699.

[94] *Id.*

[95] *Id.*

[96] *See id.* at 698-99.

Notably, the Court held that seizure of a traveler's luggage is "tantamount to seizure of the person."[97] Applying the *Terry v. Ohio*[98] balancing of interests approach (balancing the government interest with the degree of intrusion),[99] the *Place* Court held that the law enforcement conduct "exceeded the permissible limits of a *Terry*-type investigative stop."[100] While *Terry* permitted law enforcement to seize Place and his luggage in a limited way based merely upon reasonable suspicion, the conduct of the agents here rose to a higher level requiring probable cause. Since probable cause was not present, the seizure was "unreasonable."[101] The length of the detention of the bags until the dog sniff—ninety minutes—was not reasonable given that the agents failed to act diligently when they could have. They knew that the defendant was coming to New York and they could have had the dog at the airport of arrival. While the Court "decline[d] to adopt any outside time limitation," the ninety-minute period here was too long.[102]

In evaluating whether a legally permissible reasonable suspicion limited seizure had converted into a more significant seizure requiring probable cause, the *Place* Court emphasized (1) the movement of the luggage, (2) the length of the detention of the luggage, and (3) whether law enforcement diligently pursued their investigation.[103] How do those concerns apply in the context of the eleven-day seizure and retention of Abidor's laptop? Significantly, the *Place* case does not occur at the border.[104] As such, the Court might simply decide that the case is wholly inapplicable. If they do consider *Place*, however, it helps Abidor in several ways. First, the *Place* Court treated the seizure of the luggage as "tantamount to seizure of the person,"[105] which obviously helps Abidor in his argument that seizing and searching his laptop is more akin to a person than it is to property. Second, whereas *Place* viewed the situation as one where the seizure had converted from a reasonable suspicion seizure into a probable cause seizure, Abidor's situation could be viewed as one that progressed from needing no individualized suspicion to needing reasonable suspicion. CBP agents moved the laptop, held it for an extended period of time, and, arguably, did not diligently pursue their investigation.

---

[97] *Id.* at 708 n.8.

[98] 392 U.S. 1 (1968).

[99] *Place,* 462 U.S. at 703.

[100] *Id.* at 709.

[101] *Id.* at 710.

[102] *Id.* at 709.

[103] *See id.* at 707-10; *see also* Florida v. Royer, 103 S. Ct. 1319, 1329 (1983); Dunaway v. New York, 442 U.S. 200 (1979).

[104] *Place,* 462 U.S. at 698.

[105] *Id.* at 708 n.8.

Lastly, in *City of Ontario, California v. Quon*, the Court considered whether a government employer violated the rights of an employee when the employer read text messages sent and received on a pager the employer issued to the employee.[106] The Court assumed, for argument's sake only, that the employee had a reasonable expectation of privacy over text messages sent on the government-provided pager.[107] Nevertheless, the Court decided that the conduct of the employer, *under the circumstances*, was reasonable.[108]

The *Quon* Court, however, refused to conclude that there is always a reasonable expectation of privacy over electronic communication and devices:

> The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. . . . Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . . A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds.[109]

Based upon *Quon*, it seems that the Supreme Court will decide questions involving advanced forms of technology on a case-by-case basis. If facing a situation like that presented in *Abidor*, will the Court fully embrace the personal privacy concerns at issue with electronic devices at the border? Or will it figure out a way to resolve Abidor's matter on very narrow grounds (or not review it at all)? Will the fear of "elaborating too fully on the Fourth Amendment implications" of laptop searches at the border chill the Supreme Court? If the decision was up to Justice Scalia, it seems he would face the question directly—regardless of the presence of an advanced form of technology. In his *Quon* concurrence, Justice Scalia urges the Court to draw the digital line:

---

[106] 130 S. Ct. 2619, 2624-26 (2010).

[107] *See id.* at 2628-31.

[108] *See id.* at 2632-33.

[109] *Id.* at 2629-30.

> Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice. The Court's implication that where electronic privacy is concerned we should decide less than we otherwise would (that is, less than the principle of law necessary to resolve the case and guide private action) – or that we should hedge our bets by concocting case-specific standards or issuing opaque opinions – is in my view indefensible. The-times-they-are-a-changin' is a feeble excuse for disregard of duty.[110]

Will Justice Scalia be the force that empowers the Court to rule on laptop searches at the border?

IV. OTHER RELEVANT CONSIDERATIONS

A. General Reflections on Justices of the Supreme Court

Analyses of political science databases by the *New York Times* reflect that the Roberts Court "has staked out territory to the right of the two conservative[111] courts that immediately preceded it," noting that "[i]n its first five years, the Roberts court issued conservative decisions 58 percent of the time. And in the term ending a year ago, the rate rose to 65 percent, the highest number in any year since at least 1953."[112] The *New York Times* article further notes:

---

[110] *Id.* at 2635 (Scalia, J., concurring) (citation omitted).

[111] What does "conservative" mean in the context of the *New York Times* article?

> The leading database, created by Harold J. Spaeth with the support of the National Science Foundation about 20 years ago, has served as the basis for a great deal of empirical research on the contemporary Supreme Court and its members. In the database, votes favoring criminal defendants, unions, people claiming discrimination or violation of their civil rights are, for instance, said to be liberal. Decisions striking down economic regulations and favoring prosecutors, employers and the government are said to be conservative.

Adam Liptak, *Court Under Roberts Is Most Conservative in Decades*, N.Y. TIMES, July 25, 2010, at A1, *available at* http://www.nytimes.com/2010/07/25/us/25roberts.html?_r=

> Four of the six most conservative justices of the 44 who have sat on the court since 1937 are serving now: Chief Justice Roberts and Justices Alito, Antonin Scalia and, most conservative of all, Clarence Thomas. (The other two were Chief Justices Burger and Rehnquist.) Justice Anthony M. Kennedy, the swing justice on the current court, is in the top 10.[113]

As for the additions of Elena Kagan and Sonia Sotomayor, the article notes that "there is no reason to think they will make a difference in the court's ideological balance. Indeed, the data show that only one recent replacement altered its direction, that of Justice Samuel A. Alito, Jr. for Justice Sandra Day O'Connor in 2006, pulling the court to the right."[114]

The current political composition of the Court (five Justices nominated by Republican presidents and four Justices nominated

---

1&scp=1&sq=%22Court%20Under%20Roberts%20is%20most%20conservative%20in%20decades&st=cse.

[112] *Id.*

[113] *Id.*

[114] *Id.*; *see also* Greg Stohr, *Roberts Supreme Court's Partisan Split Shows New Justices Are Predictable,* BLOOMBERG.COM (June 30, 2011, 11:01 PM), http://www.bloomberg.com/news/2011-07-01/roberts-supreme-court-s-partisan-split-shows-new-justices-are-predictable.html ("The newest justices fueled the trend, rewarding the men who appointed them with consistent and predictable votes. President Barack Obama's two choices, Sonia Sotomayor and Elena Kagan, voted in virtual lockstep and usually alongside fellow Democratic appointees Ruth Bader Ginsburg and Stephen Breyer. Former President George W. Bush's two selections, Chief Justice John Roberts and Justice Samuel Alito, voted together more than any other duo."). *But see* Joan Biskupic, *"Dynamic" duo of Kagan, Sotomayor add vigor to court*, USA TODAY (Mar. 1, 2011, 1:46 PM), http://www.usatoday.com/news/washington/judicial/2011-03-01-courtarguments_N.htm ("The new justices have brought a stronger voice on the left than the four liberals had before Sotomayor joined on 2009 and Kagan in 2010. Kagan particularly is putting forward broader legal arguments that could guide her colleagues' thinking, often in contrast to those set up by the court's five conservatives.").

by Democratic presidents)[115] and the studies referenced here suggest that any decision in Abidor's case would favor the government—likely ruling that a laptop is mere property and that it can be searched at the border and beyond without reasonable suspicion. On the other hand, national security concerns do not fall neatly into ordinary political divisions—will politics or ideological perspectives have any impact? While, "by and large, presidents are successful with their appointees" with respect to desired ideological goals,[116] Supreme Court history reveals instances of Justices deciding cases wholly inconsistent with the perspective that the public, and the president who appointed the justices, might have anticipated.[117] The answer is not clear—but it does appear that the present composition of the United States Supreme Court will favor the government in any ruling on searching electronic devices at the border.

B. Perspectives of Justices in Various Oral Arguments

What guidance can be obtained from the questions and comments from the Justices at oral argument? Of course, a Justice's words at oral argument have no persuasive value under the law—but they can be very revealing when speculating how a Justice might respond in future situations. This Section will examine the words of various Justices[118] in the oral arguments from the border search case, *United States v. Flores-Montano*,[119] and the advanced technology case of *City of Ontario, California v. Quon*.[120]

---

[115] *See Biographies of Current Justices of the United States*, UNITED STATES SUPREME COURT, http://www.supremecourt.gov/about/biographies.aspx (last visited Jan. 23, 2012).

[116] LEE EPSTEIN & JEFFREY A. SEGAL, ADVICE AND CONSENT: THE POLITICS OF JUDICIAL APPOINTMENTS 132 (2005).

[117] Bradley W. Joondeph, *Law, Politics, and the Appointment Process*, 46 SANTA CLARA L. REV. 737, 751 (2006) ("Earl Warren and William Brennan had voting records that were much more liberal than the views of Dwight Eisenhower. Byron White was substantially more conservative than John F. Kennedy. Harry Blackmun grew more liberal than Richard Nixon, and David Souter's voting record has likely surprised George H.W. Bush. Nonetheless, '[m]ost justices appointed by conservative presidents cast a high percentage of conservative votes,' while 'most justices appointed by liberal presidents cast a higher percentage of left-of-center votes than their colleagues seated by more conservative presidents.' That is, '[m]ore often than not' justices 'vote in ways that would very much please the men who appointed them.'" (quoting EPSTEIN & SEGAL, *supra* note 116, at 132)).

[118] This Section will not consider the comments or questions of Justice Clarence Thomas because he has not spoken at oral argument in over five years. *See* Adam Liptak, *No Argument: Thomas Keeps 5-Year Silence,* N.Y. TIMES, Feb. 13, 2011, at A1,

1. *United States v. Flores-Montano*

In *Flores-Montano*, Justice Breyer suggests that he is concerned with the potential for overzealous agents at the border. Consider the following:

> I'm trying to figure out if we have each customs agent for himself to conduct whatever suspicionless searches he wants, and you have a few of the, perhaps in every organization there are a few unusual ones who cause some problems, are there any internal checks within the system, because you're going to not have a judicial check?[121]

Justice Breyer appears to be concerned that there is not enough oversight, especially judicial oversight, with the conduct of federal agents at the border. Does this indicate he might be supportive of requiring law enforcement to have some kind of individualized suspicion to examine the contents of electronic devices at the border? In his concurrence in *Flores-Montano*, he makes note of the fact that CBP keeps records of border searches it conducts (including the reasons for the searches).[122] Will those records satisfy the oversight concerns of Justice Breyer?

In questioning counsel for Flores-Montano, Justice Breyer voices concern with the implications of empowering terrorist

---

available at http://www.nytimes.com/2011/02/13/us/13thomas.html?_r=1 ("A week from Tuesday, when the Supreme Court returns from its midwinter break and hears arguments in two criminal cases, it will have been five years since Justice Clarence Thomas has spoken during a court argument."); *see also* David A. Karp, *Why Justice Thomas Should Speak at Oral Argument*, 61 FLA. L. REV. 611, 612-13 (2009) ("Since 2004, when oral argument transcripts began identifying Justices by name, Justice Thomas has made just eleven comments—while sitting through more than 400 hours of argument.").

[119] 541 U.S. 149 (2004).

[120] 130 S. Ct. 2619 (2010).

[121] Oral Arg. at 22:8-15 United States v. Flores-Montano, 541 U.S. 149 (2004) (No. 02-1794) [hereinafter *Flores-Montano* Oral Argument], *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/02-1794.pdf (last visited Jan. 23, 2012).

[122] *Flores-Montano*, 541 U.S. at 156 (Breyer, J., concurring).

activity if reasonable suspicion is required for disassembly of property:

> [S]uppose there's a terrorism problem and . . . they say that we want to search every fifteenth truck that comes in, there might be anthrax or bombs or whatever and we want to give the agents the power to look thoroughly into these big trucks even without suspicion. Now were you saying the Fourth Amendment would stop that?[123]

Would Justice Breyer be similarly concerned if the "property" in question was a laptop or some other kind of electronic device? The potential for enabling terrorism is present in either situation. How will Justice Breyer and the Court balance terrorist concerns with the privacy of individuals like Pascal Abidor?

Justice Scalia is also concerned with burdening agents at the border: "[T]here are just some intuitions that agents get that may not rise to the level of what a court may acknowledge is an articulable suspicion, and they shouldn't—they shouldn't have to worry about whether they have to prove that or not."[124] Justice Scalia seems to have confidence in the intuition of agents—as such, they should not have to worry about whether or not they have sufficient individualized suspicion. As for the oversight concerns brought up by Justice Breyer, Justice Scalia offers the following comment:

> I mean, it seems to me if you have an agent who repeatedly has a—cars backing up at the—at the gate that—that he's controlling, and who repeatedly comes up empty on—on gas tank searches, that fellow's not going to be there very long. I mean, it, it's easy to observe somebody who's abusing the system, it seems to me.[125]

Justice Scalia appears to think that overzealous federal agents will be rare because the open nature of their job will prevent them from abusing their power. Given his comments, it seems unlikely that Justice Scalia would be sympathetic to any argument presented by Pascal Abidor.

---

[123] *Flores-Montano* Oral Argument, *supra* note 121, at 40:2-10.

[124] *Id.* at 36:4-7.

[125] *Id.* at 37:5-11.

What about Justice Kennedy, often referred to as the "swing vote"[126] with the present Supreme Court? Does he give any indication of his perspective in the *Flores-Montano* oral argument? Consider the following comments:

> If 85 percent of the people with the gas tanks that were searched have the contraband, what you're asking us to do is to protect the expectation of the other 15 percent . . . it seems to me to put the exclusionary rule somewhat into question with reference to the border.[127]

Is Justice Kennedy suggesting that the ends should justify the means? The implication is that the large majority of time the agents get the bad guy—so the remaining fifteen percent of the public should just deal with it. Will Justice Kennedy feel the same way about Pascal Abidor?

2. *City of Ontario, California v. Quon*

What about the Court's comfort level with advanced forms of technology? Might that have an impact on how they constitutionally approach searches at the border when electronic devices are at issue? A review of a few passages from the *Quon* oral argument is revealing.

Consider a few comments and questions of Chief Justice Roberts:

> And I think it might be the better course to say that the Constitution applies, but we're going to be more flexible in

---

[126] *See* Adam H. Morse & Julian E. Yap, *A Panel-Based Supreme Court*, 37 OHIO N.U. L. REV. 23, 34-35 (2011) ("The frequency with which the Court decides cases by a 5-4 vote with at most one or two swing Justices – often O'Connor before her retirement and Kennedy since then—creates a reality that the law, particularly on matters of constitutional law, is frequently whatever one swing Justice says it is. For example, the Court split 5-4 or 6-3 in almost half of the seventy-four signed decisions over the course of the 2008 October Term. Justice Kennedy was in the majority 92% of the time, and, crucially, in all but five of the twenty-three cases that split 5-4." (footnote omitted)); *see also* Erwin Chemerinsky, *When it Matters Most, it is Still the Kennedy Court*, 11 GREEN BAG 2D 427, 427-28 (2008) ("The bottom line is that when the Court is divided 5-4 on issues where there are clear liberal and conservative positions, Justice Kennedy is the swing vote.").

[127] *Flores-Montano* Oral Argument, *supra* note 121, at 50:18-24.

> determining what's reasonable because they are dealing with evolving technology . . . .[128]
>
> . . .
>
> . . . I just don't know how you tell what is reasonable—I suspect it might change with how old people are and how comfortable they are with technology . . . .[129]
>
> . . .
>
> . . . Maybe—maybe everybody else knows this, but what is the difference between a pager and e-mail?[130]

Chief Justice Roberts is obviously wary about giving constitutional status to a particular type of technology because technology changes so fast. What does it mean to "be more flexible in determining what's reasonable because they are dealing with evolving technology"? One could infer from this statement that Justice Roberts thinks law enforcement should be given wider discretion when dealing with advanced forms of technology—after all, since technology is changing so rapidly, it is reasonable for law enforcement in exploring advanced forms of technology to periodically make some reasonable mistakes.

What about his comments regarding age and comfort with technology? Chief Justice Roberts seems to be saying that age and experience can help shape one's perspective on the "reasonableness" of the expectation of privacy in regards to electronic devices. Assuming he is not particularly comfortable with technology, could one expect that he might conclude that a heightened expectation of privacy in an electronic device at the border is not reasonable? Hence, the intrusion on a person like Mr. Abidor is not that high?

What about Chief Justice Roberts's question about the difference between a pager and e-mail—does this offer any guidance? His lack of understanding of technology[131] might impact how bold the Court will be when reviewing new technology in future decisions. He might conclude that the best course of action is to simply leave the issues to the lower courts and let the passage of time resolve the constitutional issues presented by the technology.

---

[128] Oral Arg. at 23:7-11 City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (2010) (No. 08-1332) [hereinafter *Quon* Oral Argument], *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/08-1332.pdf (last visited Jan. 26, 2012).

[129] *Id.* at 24:1-4.

[130] *Id.* at 29:18-20.

Justice Scalia also offers some interesting comments. Recall that the *Quon* case considered whether a public employer violated the rights of an employee when the employer read text messages sent and received on a pager the employer had issued to the employee. In the following passage, Justice Scalia discusses the role of the statute, the Stored Communications Act,[132] in relation to the Fourth Amendment: "[T]hat's why you have the statute, because the Fourth Amendment wouldn't solve the problem, because you are effectively making it public by sending it to somebody whom you don't know is immune from disclosure. So, in order to stop the intermediary from making it public, you needed the statute."[133] Justice Scalia is sending the clear message that the Constitution (specifically, the Fourth Amendment) cannot cover every concern; statutes may be a more appropriate means for fully protecting digital information than the Fourth Amendment. Does this suggest he might want to stay the course with laptops at the border—continuing to allow full searches without any individualized suspicion? Would he leave it to Congress—if they deem it appropriate—to provide more protection to travelers at the border?

---

[131] A thorough review of the *Quon* oral argument reflects that the Court could use some guidance on modern technology and how the various devices work. *See, e.g.*, *id.* at 25:20-23 (Chief Justice Roberts: "So, your—your position would require people basically to have two of these things with them, two whatever they are, text messager or the BlackBerries or whatever, right?"); *id.* at 44:1-5 (Chief Justice Roberts: "What happens, just out of curiosity, if you're—he is on the pager and sending a message and they're trying to reach him for, you know, a SWAT team crisis? Does he—does the one kind of trump the other, or do they get a busy signal?").

[132] Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2011).

[133] *Quon* Oral Argument, *supra* note 128, at 52:14-19.

C. Potential Federal Legislation on Warrantless Border Searches of Electronic Devices

In *Cotterman*, in the context of seizing and later searching a laptop at the border, the Ninth Circuit discussed the role of courts versus the role of Congress or the executive branch:

> We recognize that few legitimate travelers would appreciate being regularly delayed in order to allow the Government to adequately search his or her property. However, our role is to determine what is legal, not what is desirable. We leave to Congress or the Department of Homeland Security the decision to promulgate limits on the utilization of more complex searches through legislation or rulemaking . . . .[134]

In fact, Congress has considered[135] and is considering legislation on warrantless border searches of electronic devices. In January 2011, Representative Loretta Sanchez (D-CA) introduced the Border Security Search Accountability Act of 2011 (2011 Border Security Act).[136] Some interesting aspects of the legislation[137] include:

---

[134] United States v. Cotterman, 637 F.3d 1068, 1077 n.10 (9th Cir. 2011).

[135] In 2008-09, Senator Russ Feingold (D-WI) and Representative Eliot Engel (D-NY) sponsored bills to statutorily require some level of suspicion to search electronic devices at the international border. Securing Our Borders and Our Data Act of 2009, H.R. 239, 111th Cong. (2009); Travelers' Privacy Protection Act of 2008, S. 3612, 110th Cong. (2008). These bills were not presented for a vote during the last session of Congress but demonstrate that Congress has been concerned with electronic border searches for several years. *See also* Carolyn James, *Balancing Interests at the Border: Protecting Our Nation and Our Privacy in Border Searches of Electronic Devices*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 219, 227-30 (2011) (discussing other legislation considered in 2008-09 as well as past and present directives of CBP and ICE). Congress has also passed legislation generally covering border searches. *See, e.g.*, 19 U.S.C. § 482 (2002).

[136] Border Security Accountability Act of 2011, H.R. 216, 112th Cong. (2011) [hereinafter 2011 Border Security Act], *available at* http://pub.bna.com/eclr/hr216intro.pdf.

[137] A detailed comparison of the 2009 CBP Directive and the 2009 ICE Directive, see *supra* note 7, with the 2011 Border Security Act, is beyond the scope of this Article. Nevertheless, it is worth noting that some of the concerns addressed in this proposed legislation are already covered in the directives. For example, the 2011 Border Security Act would require that searches of electronic devices be done in the presence of a supervisor. The 2009 CBP Directive is in accord with this recommendation. 2009 CBP

- Prohibits confidential information (e.g. medical information) viewed at the border from being shared with other government agencies;[138]
- Searches of electronic devices must be done "in presence of a supervisor and, where appropriate, in the presence of the individuals whose electronic devices are subject to searches";[139]
- Ascertain a set number of days electronic devices can be retained by border officials absent "probable cause";[140]
- Those who have data copied, retained, shared, or entered given written notice unless that hinders a national security investigation;[141]
- Individuals receive receipt if electronic device taken from them;[142]
- Proper training on privacy, civil rights, etc., to each officer conducting searches of electronic devices at the border;[143]
- Auditing mechanism to ensure proper procedure taken for e-device searches.[144]

DIRECTIVE, *supra* note 7, § 5.1.3. The 2009 ICE Directive, however, does not have such a requirement. *See* 2009 ICE DIRECTIVE, *supra* note 7.

[138] 2011 Border Security Act, *supra* note 136, § 2(b)(2).

[139] *Id.* Both the 2009 CBP Directive and the 2009 ICE Directive include language suggesting that the searches be done in the presence of the traveler, but the exceptions to this exception are very broad. *See, e.g.*, 2009 CBP DIRECTIVE, *supra* note 7, § 5.1.4 ("Searches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, or other operational considerations that make it inappropriate to permit the individual to remain present."); 2009 ICE DIRECTIVE, *supra* note 7, § 8.1(2) ("If permitting an individual to witness the search itself could reveal law enforcement techniques or potentially compromise other operational concerns, the individual will not be permitted to observe the search.").

[140] 2011 Border Security Act, *supra* note 136, § 2(b)(3).

[141] *Id.* § 2(b)(6).

[142] *Id.* § 2(b)(5).

[143] *Id.* § 3(a).

[144] *Id.* § 3(b). While Congress considers legislation like the 2011 Border Security Act, it simultaneously contemplates laws that go in the opposite direction. *See, e.g.*,

There is clearly some public support to limit the government's role at the border.[145] For example, on May 18, 2011, an advocacy group called The Constitution Project issued a report describing various legal and privacy concerns with DHS's border search policies with regard to electronic devices.[146] Reporters are routinely highlighting the experiences of individuals who have encountered electronic problems at the border.[147] Simultaneously, however, national security interests are highlighted almost

---

David Kravets, *Internet 'Kill Switch' Legislation Back in Play*, WIRED.COM (Jan. 28, 2011), http://www.wired.com/threatlevel/2011/01/kill-switch-legislation/ ("Legislation granting the president internet-killing powers is to be re-introduced soon to a Senate committee . . . . An aide to the Homeland Security committee described the bill as one that does not mandate the shuttering of the entire internet. Instead, it would authorize the president to demand turning off access to so-called 'critical infrastructure' where necessary.").

[145] *See* Alan Charles Raul Washington, Letter to Editor, *Time to Revive Privacy Board to Protect Civil Liberties,* N.Y. TIMES (Nov. 22, 2010), http://www.nytimes.com/2010/11/23/opinion/lweb23privacy.html (In light of "the intrusiveness of laptop searches at the border," the author calls for President Obama to revive the Privacy and Civil Liberties Board which has been vacant since January 2008: "The privacy board was originally enacted in response to a recommendation of the 9/11 Commission to help ensure that the war against terrorism would not compromise the rights of Americans.").

[146] *See* THE CONSTITUTION PROJECT, SUSPICIONLESS BORDER SEARCHES OF ELECTRONIC DEVICES: LEGAL AND PRIVACY CONCERNS WITH THE DEPARTMENT OF HOMELAND SECURITY'S POLICY (2011) [hereinafter THE CONSTITUTION PROJECT], http://www.constitutionproject.org/pdf/Border_Search_of_Electronic_Devices_0518_2011.pdf.

[147] *See, e.g.*, Shahrzad Noorbaloochi, *Legality of Homeland Security Searches of Electronics at Border Questioned*, THE EPOCH TIMES (Feb. 7, 2011), http://www.theepochtimes.com/n2/content/view/50744/ ("David House, 23, of Cambridge, Mass., is an MIT researcher whose laptop, flash drives, and cameras were confiscated at the U.S.-Mexico border by the Department of Homeland Security (DHS) on his way back into the United States after a vacation in Mexico."); Kim Zetter, *Another Hacker's Laptop, Cellphones Searched at Border*, WIRED.COM (Nov. 18, 2010 8:25 PM), http://www.wired.com/threatlevel/2010/11/hacker-border-search ("A well-known and respected computer-security researcher was detained for several hours Wednesday night by border agents who searched his laptop and cell phones before returning them to him."). Zetter's article suggests that some of the people detained might have had a connection to Wiki Leaks. While some might support the publication of top-secret federal government data, as Wiki Leaks promotes, there is arguably a parallel fear that those who facilitate the exposure of such documents on the Internet are a danger to national security. Since websites like Wiki Leaks are dependent upon the passage of information via electronic devices, Congress might experience some strong political pressure to not pass legislation that would afford additional protections at the border.

daily.[148] Is the 2011 Border Security Act the most that can be expected in light of the significant national security interests involved with border searches?[149] Does it sufficiently address the privacy intrusion involved with this type of search?

Notably, the 2011 Border Security Act does not address one of Abidor's main concerns—the detailed search of an electronic device without reasonable suspicion. Neither the 2009 CBP Directive nor the 2009 ICE Directive require individualized suspicion to search electronic devices.[150] One recommendation in The Constitution Project's report urges DHS to "[a]mend the CBP and ICE Directives to require that CBP and ICE officials may not search the content or information contained in electronic devices of U.S. persons unless there exists a reasonable suspicion that the electronic device contains illegal material or evidence of illegal conduct."[151]

The 2011 Border Security Act would require DHS to ascertain a set number of days electronic devices can be retained by border officials absent "probable cause."[152] In contrast, under both the 2009 CBP Directive and the 2009 ICE Directive, agents may detain electronic devices for further review for a "reasonable" period of time.[153] The 2009 CBP Directive specifically states that "[u]nless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days."[154] The 2009 ICE Directive states that "[s]earches are generally to be completed within 30 days of the date of detention, unless circumstances exist that would warrant more time."[155]

---

[148] *See, e.g.*, Eric Schmitt, *Lawmakers Hear of Threat by Domestic Terrorists*, N.Y. TIMES, Feb. 10, 2011, at A14, *available at* http://www.nytimes.com/2011/02/10/us/politics/10terror.html?ref=politics ("'In some ways, the threat today may be at its most heightened state since the attacks nearly 10 years ago,' Janet Napolitano, the secretary of homeland security, told lawmakers.").

[149] As of the writing of this Article, Congress had not acted on this bill after referring it to the House Committee on Homeland Security.

[150] *See* 2009 ICE DIRECTIVE, *supra* note 7, § 6.1; 2009 CBP DIRECTIVE, *supra* note 7, § 5.1.2.

[151] THE CONSTITUTION PROJECT, *supra* note 146, at 11.

[152] 2011 Border Security Act, *supra* note 136, § 2(b)(3).

[153] 2009 ICE DIRECTIVE, *supra* note 7, § 8.3(1); 2009 CBP DIRECTIVE, *supra* note 7, § 5.3.1.

[154] 2009 CBP DIRECTIVE, *supra* note 7, § 5.3.1.

[155] 2009 ICE DIRECTIVE, *supra* note 7, § 8.3(1).

What impact might public opinion and pending legislation have on the courts, and possibly the Supreme Court, when facing facts like that presented in the *Abidor* case? It may motivate the courts to "stay the course," giving law enforcement wide authority at the border as has been the case for decades. If Congress wants to give travelers greater protection than the Supreme Court's interpretation of the Constitution requires, it can do so. Courts may choose to dodge the issue and let the legislature address—if they desire to do so—the privacy concerns presented by these border searches.

D. Fourth Amendment and First Amendment Concerns at the Border

In the context of border searches, a high potential exists for conflict between law enforcement authority under the Fourth Amendment and the right to free expression under the First Amendment. The Court, however, has not been very sympathetic to First Amendment concerns at the border, as noted in the 1972 *Ramsey* decision: "More fundamentally, however, the existing system of border searches has not been shown to invade protected First Amendment rights . . . ."[156] The Court's comments in *Ramsey—focusing* on the "existing system of border searches"—seem to leave open the possibility that the Court might consider the First Amendment concerns under a *different* system of border searches.[157] Do border searches of electronic devices present that opportunity? As one academic authority noted in 2010:

---

[156] United States v. Ramsey, 431 U.S. 606, 623 (1977).

[157] *See* Timothy Zick, *Territoriality and the First Amendment: Free Speech at—and Beyond—Our Borders*, 85 NOTRE DAME L. REV. 1543, 1568 (2010) ("In *United States v. Ramsey*, the Supreme Court held that the probable cause and warrant requirements did not apply to the opening of incoming international letter-class mail by customs officials. Such searches were deemed reasonable merely by virtue of their location. The *Ramsey* Court summarily dismissed any First Amendment concerns, reasoning that the detailed regulatory restrictions on opening letter mail negated any concern regarding the chilling of expression. 'Accordingly,' the Court said, 'we find it unnecessary to consider the constitutional reach of the First Amendment in this area in the absence of the existing statutory and regulatory protection.' *Ramsey* thus declined an invitation to de-territorialize constitutional scrutiny of border searches involving expressive materials. The invitation has recently been proffered anew—and again declined—in cases involving more modern forms of communication.").

> The era of the personal computer has raised some new concerns regarding the territorial First Amendment. In a globalized society, international travelers routinely carry computing devices, which are typically filled with expressive material, at the border. The question has arisen whether the First Amendment requires an exception to the broad search and seizure authority customs officials possess at the nation's borders. . . . Although most of the constitutional concerns regarding border searches relate to the Fourth Amendment, serious First Amendment issues can also arise. As we have seen, information and ideas flow across the border in many different forms. . . . Laptops and other computing devices now routinely carried by international travelers contain private and expressive material including diaries, medical information, personal correspondence, and financial records. Travelers subjected to warrantless border searches have challenged the searches on both Fourth Amendment and First Amendment grounds.[158]

Despite the Court's apparent lack of concern about First Amendment issues at the border, "[t]ravelers subjected to warrantless border searches have challenged the searches on both Fourth Amendment and First Amendment grounds."[159] In general, however, lower courts have chosen not to recognize any First Amendment exception to the broad border search authority.[160] To hold otherwise, say the lower courts, would "create a sanctuary at the border for all expressive material—even for terrorist plans . . . ." Furthermore, recognizing a First Amendment exception to the border search doctrine would ensure significant headaches for those forced to determine its scope and "[t]hese sorts of legal wrangles are exactly what the Supreme Court wished to avoid by sanctioning expansive border searches."[161]

Given the present state of the law, it appears that any First Amendment claims presented by Abidor are not likely to be well-received.[162] The national security concerns and the administrative problems presented by increased scrutiny may simply be too great. Will the same problems limit travelers' Fourth Amendment protections at the border?

---

[158] *Id.* at 1567-68.

[159] *Id.* at 1568.

[160] *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1010 (9th Cir. 2008); United States v. Ickes, 393 F.3d 501, 506-07 (4th Cir. 2005).

[161] *Ickes*, 393 F.3d at 506.

E. Frequency of Border Searches of Electronic Storage Devices

Do lawsuits like Abidor's overstate the problems regarding border searches of electronic devices? Is there really a problem with border searches of these devices? It helps to review some raw numbers on actual border searches.

According to Abidor's complaint, "[b]etween October 1, 2008, and June 2, 2010, over 6500 people—nearly 3000 of them U.S. citizens—were subjected to a search of their electronic devices as they crossed U.S. borders."[163] On its face, this seems like a lot of potential privacy intrusions.

The Department of Homeland Security, however, provides a different perspective using very similar numbers:

> For the reporting period October 1, 2009 to April 30, 2010, CBP encountered more than 168.2 million travelers at U.S. ports of entry. Of these travelers, approximately 3.7 million (2.2% of the 168.2 million travelers) were referred for secondary inspection; however, of these 3.7 million travelers, CBP conducted *only* 2,272 searches of electronic media during this time period. A "search" in this regard is broadly defined to include a simple request to turn the device on as a means of ensuring that it is what it purports to be. Detailed information on these searches is only available for those performed on laptops. Of the total number of searches of electronic media, *only* 673 searches of any type were performed on laptops—*just* 0.0184% of

---

[162] *See* Zick, *supra* note 157, at 1570 ("In this context, at least, it is apparent that globalization and digitization have not altered the territorial First Amendment. Expressive interests are enforced differently, if at all, at the territorial borders. Like other border searches, warrantless and suspicionless searches of computing devices have been deemed valid merely by virtue of their location. This is so despite the fact that the search of computing devices is in some cases a more substantial invasion than, say, a search of papers or international mail.").

[163] Abidor Complaint, *supra* note 4, at 1.

> the 3.7 million travelers referred to secondary inspection.[164]

Is that right? Only 0.018 percent of travelers had their laptops searched? That doesn't seem like much of a problem.

Upon examination, Abidor's numbers and the DHS numbers are not inconsistent with each other. According to Abidor's figures, over twenty months, 6500 electronic storage devices were searched; according to the DHS figures, over seven months, 2272 electronic storage devices were searched. Using some simple math, Abidor's figures result in 325 searches per month and the DHS figures reflect 324.6 searches per month—out of the approximate 530,000[165] travelers referred to secondary searches each month.

Obviously, the figures reflect a sufficient enough number of searches that privacy advocates are concerned—but will the courts pay attention? Are the numbers so low that courts might overlook the potential problem due to broader concerns about national security interests?[166] The fact that DHS is keeping track of the searches might be enough to minimize the concern that the privacy rights of individuals are being affected. Maybe Abidor's situation is unique—the figures suggest that the average American is not likely to have any problems with border searches of electronic devices.

F. Impact of Encryption

Should customs agents seize an electronic device if they cannot read the data in it? If they do seize it, how long can they keep it in an effort to uncover the data? Seemingly, it does little good for CBP or ICE to seize an electronic device if they cannot do anything with it. Assuming they do seize it, how long can they reasonably hold and examine the device? Does the mere fact that the agents detect that the device possesses encrypted data give agents reasonable suspicion that crime is afoot, thus mooting any concerns about potential Fourth Amendment violations?

---

[164] DEPARTMENT OF HOMELAND SECURITY PRIVACY OFFICE, ANNUAL REPORT TO CONGRESS JULY 2009–JUNE 2010 at 49 (2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2010.pdf (emphasis added).

[165] This figure was obtained by doubling the DHS figure of 3.7 million travelers referred to secondary searches over a six-month period of time, and then dividing that figure by twelve months.

[166] *See supra* notes 126-27 and accompanying text (reflecting on Justice Kennedy and the potential for overlooking a small problem to prevent a much larger problem).

"[E]ncryption is the process of transforming information . . . using an algorithm . . . to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key."[167] Given the pressing demands at the border, the average CBP or ICE agent is not likely to possess that "special knowledge." Are agents likely to see electronic devices utilizing encryption as a means to protect the privacy of data?

Will travelers use programs like TrueCrypt—"Free open-source on-the-fly encryption"[168]—freely available to anyone interested in using it? Truecrypt.org even offers "step-by-step instructions on how to create, mount, and use a TrueCrypt volume"[169]—so even beginners can use their product.

Assuming a traveler uses encryption and law enforcement wants to be able examine the electronic data of the traveler, will law enforcement be able to crack it? Will the law enforcement officer examining the electronic device even be able to know that an encrypted partition of the hard drive exists? Assuming the following comments to be accurate, encryption presents agents with a serious problem. Not only is it likely that agents won't be able to access the data, they might not even be able to know that the data is encrypted:

> The FBI has admitted defeat in attempts to break the open source encryption used to secure hard drives seized by Brazilian police during a 2008 investigation. . . . Brazilian reports state that two programs were used to encrypt the drives, one of which was the popular and widely-used free open source program TrueCrypt. Experts in both countries apparently spent months trying to discover the passphrases using a dictionary attack, a technique that involves trying out large numbers of possible character

---

[167] *StorageCraft Knowledge Base: Encryption*, STORAGECRAFT http://www.storagecraft.com/kb/glossary.php?letter=E (last visited Jan. 24, 2012); *see also Definition: Encryption*, SEARCHSECURITY.COM, http://searchsecurity.techtarget.com/definition/encryption (last visited Jan. 24, 2012).

[168] TRUECRYPT, http://www.truecrypt.org/ (last visited Jan. 24, 2012).

[169] *Beginner's Tutorial*, TRUECRYPT.ORG, http://www.truecrypt.org/docs/?s=tutorial (last visited Jan. 24, 2012).

> combinations until the correct sequence is found. Brazilian reports mention that the authorities had no means of compelling the makers of TrueCrypt to help them though it is hard to see how its creators could have helped. If a complex passphrase has been used – a random mixture of upper and lower case letters with numbers and special ASCII characters throw in – and the bit length is long, formidable computing power and time would be required to chance upon the correct passphrase. TrueCrypt also uses what is termed a "deniable file system" approach to encrypting whole hard drives. *Under this design, the existence of the encrypted partition will not be obvious to anyone examining the drive[,] allowing the individual using such encryption to plausibly deny its existence.*[170]

If the criminal transports his illicit data on electronic devices at the border[171] and uses some kind of encryption, it seems possible that the CBP agents might not even be able to recognize that the data is encrypted. If the CBP agents do recognize that encryption is in place, what should they do?[172] How long can they hold the electronic devices for further examination? Encryption does not leave the agents in a good place. It appears that when TrueCrypt is used on a laptop, it would be nearly impossible to either break into the laptop or to detect it on a user's hard drive at currently available technological standards.

---

[170] John E. Dunn, *FBI hackers fail to crack TrueCrypt,* TECHWORLD.COM, (June 30, 2010 10:55 AM), http://news.techworld.com/security/3228701/fbi-hackers-fail-to-crack-truecrypt/ (emphasis added).

[171] Who is likely to transport their illegal items on electronic devices at the border? Will the really bad guys—the terrorists—do it this way? There are certainly more private (i.e., not exposed to CBP agents) electronic methods for transferring electronic data from one place to another. Tech-savvy criminals will likely use another method. If that is accurate, it seems like the CBP and ICE policies regarding searches of electronic data will only catch the non-tech-savvy criminals and those so attached to their illicit data—like child pornography collectors—that they don't want to give up possession of it. *See* KENNETH V. LANNING, NAT'L CTR. FOR MISSING AND EXPLOITED CHILDREN, CHILD MOLESTERS: A BEHAVIORAL ANALYSIS—FOR PROFESSIONALS INVESTIGATING THE SEXUAL EXPLOITATION OF CHILDREN 91 (5th ed. 2010), *available at* http://www.missingkids.com/en_US/publications/NC70.pdf ("No matter how much the preferential sex offender has, he never seems to have enough. He rarely throws anything away. If law enforcement has evidence an offender had a collection 5 or 10 years ago, chances are he still has the collection now – only it is larger."). Beyond that kind of criminal, who is left that the policies might impact? Only the average U.S. citizen?

[172] Can they force the possessor to give up passwords? While a detailed discussion of this subject is beyond the scope of this Article, the answer appears to likely be no, due to the Fifth Amendment privilege against self-incrimination—assuming giving up the password is deemed "evidence of a testimonial or communicative nature." Schmerber v. California, 384 U.S. 757, 761 (1966) ("We hold that the privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State

Does the fact that encryption exists as an alternative for criminals suggest that it will be reasonable for CBP agents to hold the laptops for longer periods of time?[173] The fact that CBP agents detect an encrypted volume on a laptop might add to the reasonable suspicion to justify the continued detention of the laptop. But what is this reasonable suspicion of? What "crime" is afoot?

If use of encryption becomes widespread, it may lessen the relevancy of any court ruling regarding border searches. The "smart" criminals will find another way to get their illegal data

---

with evidence of a testimonial or communicative nature, and that the withdrawal of blood and use of the analysis in question in this case did not involve compulsion to these ends." (footnote omitted)); *see* United States v. Kirschner, No. 09-MC-50872, 2010 WL 1257355, at *3 (E.D. Mich. Mar. 30, 2010) (forcing surrender of password violated Fifth Amendment); *In re* Boucher, No. 2:06-MJ-91, 2009 WL 424718, at *3-4 (D. Vt. Feb. 19, 2009) (finding no Fifth Amendment violation in later requiring a defendant to provide the password for an encrypted drive when the defendant had previously, post-Miranda warnings, voluntarily showed agents the encrypted drive on a laptop where child pornography was observed); *see also* John Duong, *The Intersection of the Fourth and Fifth Amendments in the Context of Encrypted Personal Data at the Border*, 2 DREXEL. L. REV. 313 (Fall 2009) (discussing *In re Boucher*, 2009 WL 424718); Susan Brenner, *Passwords and the 5th Amendment Privilege*, CYB3RCRIM3 BLOG (April 28, 2010 7:58 AM), http://cyb3rcrim3.blogspot.com/2010/04/passwords-and-5th-amendment-privilege.html.

[173] In the context of criminal search warrants for electronically stored information, Federal Rule of Criminal Procedure 41(e)(2)(B) states: "Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." Notably, due to "encryption" and other concerns, no time limit was set for later searches of electronic devices. *See* FED. R. CRIM. P. 41 advisory committee's note (2009) ("While consideration was given to a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place, the practical reality is that there is no basis for a "one size fits all" presumptive period. A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs. The rule does not prevent a judge from imposing a deadline for the return of the storage media or access to the electronically stored information at the time the warrant is issued. However, to arbitrarily set a presumptive time period for the return could result in frequent petitions to the court for additional time.").

into the United States. That might motivate the Court to simply leave the existing—suspicionless—measures in place. At least that way, CBP agents will capture the less tech-savvy criminals and it might also make the other criminals work harder to avoid detection—in the process, they might still catch a few of the "smart" ones too.

V. GENERAL REFLECTIONS

What would the Court say if the *Abidor* case, or a similar case, found its way to the Supreme Court? Given the trepidation voiced in *Quon*, the Court is not likely to go out on a limb about technology. Any decision they make would probably be decided narrowly and be consistent with the pro-government approach to border searches that the Court has exhibited in the past.[174]

If compelled from the facts of the case to rule, the Court would likely conclude, consistent with the majority of lower courts, the initial seizure and search of an electronic device is routine and no reasonable suspicion is required. The search of an electronic device is not similar to a body cavity or strip search requiring individualized suspicion; an electronic device is more like property (like the gas tank in *Flores-Montano*) and can be searched without suspicion. The search of an electronic device is not distinctly "offensive"—thus closing the window left open in *Flores-Montano* for situations that might require individualized suspicion. The typical search of an electronic device at the border would not be deemed so "destructive" as to require a different result.[175] Quite simply, an electronic device, despite the fact that it can contain vast amounts of personal information, is not an extension of the body—it is property like a piece of luggage. Additionally, as some lower courts have noted,[176] the search of an electronic device is no more offensive or destructive than a detailed search of any other property. The initial seizure and search of an electronic device will be looked at as little more than searching a piece of luggage that contains private information—an act that can be done by CBP and ICE agents without any suspicion at all.

---

[174] The Court might simply deny any petition for a writ of certiorari as was done in the *Arnold* case. United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008), *cert. denied*, 129 S. Ct. 1312 (2009).

[175] And at least at the border, convergence of the Fourth Amendment with the First Amendment will not heighten the suspicion requirement. The *Ickes* court said it best in noting that to rule otherwise would result in an administrative nightmare at the border and would create a "sanctuary" for terrorists. United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005).

[176] *See supra* notes 79-85 and accompanying text.

Why? The role of "governmental interest" is affecting the interpretation of what is "reasonable" under the Fourth Amendment. The task of a CBP agent can be daunting. The mere flow of traffic—both in cars and people—seems too heavy to require, at least immediately at the border, any kind of individualized suspicion. Requiring the presence of individualized suspicion for the initial seizure and search of electronic devices at the border would significantly lessen or eliminate the deterrent effect that the present border search policy has on criminals in bringing contraband into the United States.

Most importantly, any decision the Court would make would likely be guided by the twenty-first century's biggest national security concern—the prevention of terrorism within our country. Consider the following statement made thirteen days after September 11, 2001:

> Anyone worried about the fate of civil liberties during the U.S. government's growing war on terrorism might want to consider this Latin maxim: Inter arma silent leges. It means, "In time of war the laws are silent," and it encapsulates the supremacy of security over liberty that typically accompanies national emergencies.[177]

Are we still facing a "national emergency"? Consider the words of Janet Napolitano, secretary of DHS, nearly ten years after September 11, 2001, in addressing the House Homeland Security Committee: "In some ways, the threat today may be at its most heightened state since the attacks nearly 10 years ago."[178] Ten years have passed and the only thing that seems to have changed is an increased intrusion on personal privacy—mostly in response to the fear of terrorism that does not seem to be going away. As the sophistication of terrorist tactics increases,[179] this intrusion on personal privacy will only get worse. This national security concern will most certainly impact any court's consideration of border searches of electronic devices.[180]

---

[177] Declan McCullagh, *Why Liberty Suffers in Wartime*, WIRED.COM (Sept. 24, 2001), http://www.wired.com/politics/law/news/2001/09/47051.

[178] Eric Schmitt, *Lawmakers Hear of Threat by Domestic Terrorists*, N.Y. TIMES (Feb. 10, 2011), at A14, http://www.nytimes.com/2011/02/10/us/politics/10terror.html?ref=politics.

Is there no hope for Mr. Abidor or others like him? The time involved in retaining an electronic device for subsequent "off-site" search purposes may motivate the courts to find that reasonable suspicion of criminal evidence be present at some point. The ready availability of encryption increases the likelihood that agents will hold electronic devices for long periods of time. While in the context of a criminal case, the Court in *Place* clearly seemed troubled with law enforcement holding personal items for too long without any individualized suspicion.[181] Depending on the period of time involved, the Court might be compelled to hold that some level of individualized suspicion is necessary to hold an electronic device for further examination purposes.[182]

Assuming the Court requires reasonable suspicion of criminal activity in order to hold and examine a device beyond a particular period of time, is it going to be a tough standard for CBP and ICE agents to meet? Not likely. Time and again, the lower courts have found it unnecessary to examine the issue of whether individualized suspicion is needed because the evidence showed that reasonable suspicion was present.[183] Even if it is required, the Court has made clear that reasonable suspicion is not a hard standard for law enforcement to meet.[184]

---

[179] *See, e.g.*, Scott Shane & Robert F. Worth, *Earlier Flights May Have Been Dry Run for Plotters*, N.Y. TIMES, Nov. 1, 2010, at A14, *available at* http://www.ndtv.com/article/world/earlier-flight-may-have-been-dry-run-for-plotters-63959twrhp ("New details about the two explosive packages were disclosed by security officials in several countries, who discussed the continuing investigation on condition of anonymity. The explosive powder, pentaerythritol tetranitrate, or PETN, was found inside toner cartridges that were themselves inside HP LaserJet P2055 printers, according to officials from Germany and the United Arab Emirates.").

[180] Who will be affected if the Court allows the initial seizure and search to continue without any individualized suspicion? Certainly the child pornography possessors, since they seem to be the ones getting caught. *See supra* note 27 and accompanying text. Beyond that, the DHS statistical data seems to suggest that only a small portion of the remaining public will be affected. *See supra* note 164 and accompanying text.

[181] *See supra* notes 91-103 and accompanying text.

[182] *See supra* notes 33-65 and accompanying text (covering lower courts' discussion of the reasonableness of holding electronic devices for extended periods).

[183] *See supra* note 29 and accompanying text.

CONCLUSION

Where will the Court draw the electronic line at the international border? Consider the following from *United States v. Thirty-Seven Photographs*:

> But a port of entry is not a traveler's home. His right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during such a search. Customs officials characteristically inspect luggage and their power to do so is an old practice and is intimately associated with excluding illegal articles from this country.[185]

It appears that the "firm line" remains at the home, not with the power button for electronic devices at the border.

Pascal Abidor's tribulations certainly make a compelling story. As the American public hears about this search of electronic devices at the border, and others like it, they will certainly sympathize with seemingly innocent participants like Abidor. While the Court has periodically observed that what is "reasonable"—and their opinion of what is "reasonable"—can be affected by social customs and public beliefs,[186] this is not one of those examples. The concern for keeping our borders and our country's interior safe from terrorists and other criminals, combined with lower court and Supreme Court precedent, could prevent Abidor from ever obtaining effective and meaningful relief or leaving a lasting impression in the field of Fourth Amendment jurisprudence. Relief, if any, is likely to come from Congress.

---

[184] *See, e.g.*, United States v. Arvizu, 534 U.S. 266, 277 (2002) (holding there was reasonable suspicion present when border patrol agent observed minivan with kids set out on a "little-traveled route used by smugglers," there was a much more efficient way to travel to their alleged recreational location, the "children's elevated knees suggested the existence of concealed cargo in the passenger compartment," and the agent's assessment of the defendant's "reactions upon seeing him and the children's mechanical-like waving, which continued for a full four to five minutes"); Illinois v. Wardlow, 528 U.S. 119, 124 (2000) (finding reasonable suspicion present, which justified stop of an individual in "an area known for heavy narcotics trafficking" who exhibited "nervous, evasive behavior" and engaged in "unprovoked flight upon noticing the police"); *see also supra* notes 124-25 and accompanying text (covering comments of Justice Scalia in *Flores-Montano* oral argument and suggesting that one should rely on the intuition of agents).

[185] United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971).

[186] *See, e.g.*, Georgia v. Randolph, 547 U.S. 103, 114 (2006) ("Since the co-tenant wishing to open the door to a third party has no recognized authority in law or social practice to prevail over a present and objecting co-tenant, his disputed invitation,

In the meantime, CBP and ICE will continue to periodically turn on and look over laptops and other electronic devices without any suspicion at all. If encryption motivates the agents to retain the electronic devices for extended periods, courts might find that reasonable suspicion of criminal activity is present—but any such reasonable suspicion requirement won't be too hard to meet for the well-trained CBP agent.

People will adjust. Sophisticated criminals will encrypt more or send the data or contraband in other ways, the average citizen will transport less across international borders, and the child pornography possessors will continue to get caught because they just do not want to let go of their collection. Technology will not change how the robust Fourth Amendment applies to border searches, but it will impact how people behave at the border.

---

without more, gives a police officer no better claim to reasonableness in entering than the officer would have in the absence of any consent at all.").

THE FOURTH AMENDMENT IN A WORLD WITHOUT PRIVACY

Paul Ohm[*]

INTRODUCTION 1310
I. THE DEATH OF PRIVACY..1313
  A. The One Device 1314
  B. The Cloud 1315
  C. The Social...1316
  D. Big Data 1316
  E. The Surveillance Society 1318
II. THE DIMINISHED FOURTH AMENDMENT 1320
  A. The End of Self-Help Policing......................................1321
  B. No More Expectations of Privacy 1325
    1. Assumption of Risk 1326
    2. Knowing Exposure..1327
    3. General Public Use 1328
  C. The Inevitable Search for the New Fourth Amendment.......1329
  D. Other Solutions and Their Limits.................................1330
    1. Why Abandoning the Third-Party Doctrine Isn't Enough.....1331
    2. The Limits of Policy 1332
    3. From Privacy to Power 1334
III. THE FOURTH AMENDMENT'S THIRD ACT.....................................1336
  A. Katz *is the New* Olmstead...1336
  B. Private Power and State Action 1338
  C. Equilibrium Adjustment and the Surveillance State..........1339
    1. The Equilibrium-Adjustment Theory 1339

---

[*] Associate Professor, University of Colorado Law School. I thank the National Judicial Center and the *Mississippi Law Journal* for the invitation to participate. I specifically thank Tom Clancy for being the driving force behind this symposium, the essential annual forum for scholarly debate about the Fourth Amendment, one that deserves to continue for many years. Thanks also to Nicole Friess for research assistance.

2. The Problem with the Balance Sheet Approach ... 1341
3. New Metrics for Equilibrium Adjustment 1345
D. Beyond Warrants and Probable Cause 1347
E. Putting the Pieces Together 1351
1. The Default Rule 1351
2. Breaking the Link Between the Surveillance Society and State 1352
CONCLUSION 1353

INTRODUCTION

If we woke up tomorrow in a nation without privacy, one in which powerful companies watched the moves of every citizen, with the full awareness and consent of the watched, would the Fourth Amendment still apply? Does that amendment's "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"[1] survive once the police can request from the private sector the fruits of comprehensive, consensual private surveillance? Were we unthinkingly to extend current Fourth Amendment doctrine, the answer to these questions might be no. If we woke up tomorrow in a world without privacy, we might also find ourselves in a world without constitutional protection from new, invasive police powers. This bleak scenario is not science fiction, for tomorrow we will likely wake up in that world.

Every year, companies, especially those that deliver services online, spend millions of dollars developing new services that track, store, and share the words, movements, and even the thoughts of their customers.[2] These invasive services have proved to be irresistible to consumers, who have voluntarily embraced them in droves launching a social age of self-revelation. Millions now own sophisticated tracking devices (smartphones) studded with sensors and always connected to the Internet. They have been coaxed to use these devices to access fun and valuable services to share more information, more of the time. Our country is rapidly becoming a surveillance society.

---

[1] U.S. CONST. amend. IV.

[2] *See* discussion *infra* Part I.

Meanwhile, the police can access the records that the surveillance society produces and stores with few impediments. Current Fourth Amendment doctrine—premised on the reasonable expectation of privacy test and elaborated through principles such as assumption of risk, knowing exposure, and general public use—places far fewer hurdles in front of the police when they use the fruits of somebody else's surveillance than when they do the surveillance themselves. As the surveillance society expands, the police will learn to rely more on the products of private surveillance, and will shift their time, energy, and money away from traditional self-help policing, becoming passive consumers rather than active producers of surveillance. Private industry is destined to become the unwitting research and development arm of the FBI. If we continue to interpret the Fourth Amendment as we always have, we will find ourselves not only in a surveillance society, but also in a surveillance state.

This Article explores the relationship between private and public surveillance. In one sense, this is well-trodden ground, as many Criminal Procedure scholars have written about this relationship, especially in debates over the Fourth Amendment's third-party doctrine.[3] But few of these scholars have followed the creeping trend lines of technological evolution all the way to where they seem to be headed. Systems of private surveillance are not simply becoming more powerful and widespread, but they are becoming all-knowing and ubiquitous. What might have seemed like a slow and partial degradation of the Fourth Amendment appears instead to be a full evisceration.

But if we believe that the Fourth Amendment can and should survive the coming reach of private surveillance, it is not enough to prescribe mild tweaks to the third-party doctrine. A more thorough reinvention of the Fourth Amendment is in order. We should rebuild the Fourth Amendment atop a foundation of something other than privacy, and this Article extends the work of others who have searched for alternative theoretical underpinnings for the amendment. These scholars have convincingly suggested that the Fourth Amendment was originally intended and is better interpreted to ensure not privacy but liberty from undue government power. For more than two hundred years, privacy has served as a pretty good proxy for this value, but the rise of the surveillance society will break the connection between privacy and liberty from power and will force us to protect the core value of the Fourth Amendment through other means.

---

[3] Professor Orin Kerr quipped that "[a] list of every article or book that has criticized the [third-party] doctrine would make . . . the world's longest law review footnote." Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 n.5 (2009) (listing representative examples).

The good news is that the work of these scholars will soon take center stage, because judges are not likely to lash the Fourth Amendment to the sinking ship of privacy. The bad news is that these scholars have not yet done enough to turn their principles into concrete rules, and most importantly, they have failed to offer a workable new test to replace the venerable reasonable expectation of privacy test. Any judges convinced to shift the Fourth Amendment from privacy to liberty and power will find little in legal scholarship to help them turn their conviction into a rule.

Orin Kerr has recently offered a promising theory to fill this void. He calls it "equilibrium adjustment," the idea that Fourth Amendment rules are tailored to preserve a level playing field between the police and criminals facing technological change.[4] I embrace this theory as not only a convincing description of what courts have done but also a normatively desirable theory of what courts should do.

But I improve on Kerr's version of the equilibrium-adjustment theory, which does a good job explaining the Fourth Amendment rules that have been designed to level imbalanced, one-sided tilts in the playing field, but does not do a good job explaining what courts have done with dual-assistance technologies that aid both the police and criminals. Almost all technologies that enable new forms of private surveillance qualify as dual-assistance technologies; the telephone system, for example, helps criminals develop conspiracies outside the public sphere, but it also helps the police, by generating a detailed record of spoken conversations. Because private surveillance will soon become the most important source of information for law enforcement, Kerr's theory suffers from a serious shortcoming that needs repair.

---

[4] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

The problems with Kerr's theory are its informality and indeterminacy. Essentially, it asks judges to determine which side of the crime-fighting equation benefits more from a given technology by performing an informal accounting of the benefits and burdens to each side. To lend rigor to this approach, I recommend that judges look for hard, objective measures of how much the playing field has tilted—statistical quantities like length of investigation and number of indictments. When criminals use new private services and technologies in ways that, for example, increase the average length of police investigations, judges should relax Fourth Amendment burdens on the police. Conversely, when the police use tools to decrease the average length of investigations, judges should tighten these burdens.

This Article proceeds in three parts. Part I predicts the rise of the surveillance society and focuses, in particular, on four recent innovations: the "one device," the cloud, the social, and "Big Data." Part II explains why traditional approaches to the Fourth Amendment might give rise to a surveillance state and reviews the critiques made by others of this traditional doctrine. Finally, Part III offers a new vision for the Fourth Amendment that is designed to survive the rise of the surveillance society.

I. THE DEATH OF PRIVACY

The past decade has seen the rise of a pervasive surveillance society not that different from the one famously anticipated in 1998 by David Brin in *The Transparent Society*.[5] Brin, a noted science fiction author writing a nonfiction book, predicted a future world in which cameras peer from every street corner, wasp-sized, pilotless drones enter our bedrooms, and companies compile massive databases tracking the purchases of every consumer.[6] Today, this description sounds like a fairly conventional and entirely plausible prediction of the near future, far less extraordinary than it seemed when written.

More recently, another fiction writer, Gary Shteyngart, anticipated an equally bleak near future—but one updated to reflect an additional decade of technological innovation—in his novel *Super Sad True Love Story*.[7] In Shteyngart's dystopia, the lives of the (mostly young) New Yorkers focus on their "äppärät"; handheld devices recognizable as the offspring of today's smartphones, but smaller and sleeker, which buzz with information and constantly stream information out to the world. Not only does this make every person the potential host of a live-streaming television show about his or her life, but also it makes every social interaction an opportunity for awkward self-revelation by telling each person who walks into a bar, for example, who does (and does not) want to sleep with him, and how highly he ranks in the crowd in categories like "hotness" and "personality."[8]

---

[5] DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998).

[6] *Id.* at 3-8.

The truth is not far from the writings of these fiction writers. From among dozens of technological trends that are spurring these developments, let me focus on four: a tool, a piece of architecture, a new consumer motivation, and a class of techniques.

A. The One Device

First, consider the rise of the "one device," the convergence of a person's computing needs into a single, portable, high-powered machine, equipped with an always-on, high-speed connection to the Internet, and outfitted with dozens of sensors, including multiple digital cameras (capable of capturing still or moving images), a microphone, a GPS chip, and a digital compass.[9] Shteyngart's "äppärät" this is not, but it is close. This device knows where you are, who you are with, and what you are doing, saying, and looking at. It also sends all of this information to providers online. Today we call these devices the iPhone, iPad, and Android phone, but tomorrow they will have new names and new capabilities.

The one device enables new forms of private surveillance by giving people new modes of communication. As an already dated example, consider the text message. By giving people the ability to send short messages between phones, these devices have nearly obsoleted the short phone call and passed note.[10] Students gossip in class; spouses trade grocery lists; and employers (and drug lords) direct underlings using this relatively new medium. But as is true for all of the new technologies described in this Part, the replacement listens more and stores more than what it has replaced. Unlike the way telephone companies handle voice phone calls, text-messaging systems store copies of what is said on each endpoint and on network servers in the middle, too.[11] The one device coaxes us to communicate through it, and creates archives of what we say by default.

---

[7] GARY SHTEYNGART, SUPER SAD TRUE LOVE STORY: A NOVEL (2010).

[8] *Id.* at 90.

[9] Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 624 (2011).

B. The Cloud

Second, and closely related to the one device, is the "cloud," the migration of essential computing and storage facilities from local devices owned by users to distant servers owned by providers.[12] Companies have recognized the benefits of development, deployment, and control that come from letting users access their calendars, word-processing documents, and stored files online.

Like text messaging and the one device, the cloud opens new avenues for surveillance—consider electronic mail. Before the rise of cloud-based e-mail, people tended to use e-mail accounts provided by their employers or ISPs, and they tended to download all of their messages periodically to their personal computers, leaving no copies behind on third-party servers. With the rise of Yahoo! Mail and Hotmail in the early part of the last decade, and Gmail a few years later, millions of users now store all of their messages with third parties.[13]

---

[10] *See* PEW INTERNET & AMERICAN LIFE PROJECT, TEENS AND MOBILE PHONES (Apr. 20, 2010), *available at* http://pewinternet.org/~/media//Files/Reports/2010/PIP-Teens-and-Mobile-2010-with-topline.pdf ("Fully two-thirds of teen texters say they are more likely to use their cell phones to text their friends than talk to them by cell phone.").

[11] *See* Jacob Leibenluft, *Do Text Messages Live Forever? How a Dirty SMS Can Come Back to Haunt You*, SLATE (May 1, 2008, 6:51 PM), http://www.slate.com/id/2190382/.

[12] Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 363 (2010) (describing cloud computing).

[13] PEW INTERNET & AMERICAN LIFE PROJECT, USE OF CLOUD COMPUTING APPLICATIONS AND SERVICES (Sept. 2008), *available at* http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf (reporting that fifty-six percent

A more recent shift to the cloud has been the rise of services, like Google Docs, that provide word processing and spreadsheet handling in the cloud.[14] Before Google Docs, almost nobody systematically stored all their writings with a third party, but now some people do, and more join their ranks each week. This shift may prove even more important than the shift to cloud-based e-mail, because it exposes not only communications, but also accounting workbooks, contracts, and formal correspondence to surveillance.

C. The Social

Technical advances like smartphones and the cloud mean little if consumers choose not to adopt them. The rise of what I call "the social" has given them a reason to do so. Today's social networks—most importantly Facebook but also Twitter, Google+, and services from related companies like Zynga—build upon the innate desire of humans to want to connect to others. Software developers have realized that the simple act of allowing people to see what others are doing can trigger psychological feelings of trust and entertainment.

Once again, the rise of the social can be viewed as a boon to private surveillance. On social networks, people reveal more of their thoughts and behavior, including things they might have before chosen to hide, and to more people than they ever have before. And as with everything else that has been discussed, social networking technologies almost always store copies of all these revealed facts.

D. Big Data

The last crucial development is the rise of what some have termed Big Data, the use by companies of powerful new data analytics that help companies squeeze more value from their existing data by making inferences.[15] I have investigated some of

---

of American Internet users "use webmail services such as Hotmail, Gmail, or Yahoo! mail").

[14] *Id.* (reporting that twenty-nine percent of American Internet users "[u]se online applications such as Google Documents or Adobe Photoshop Express").

[15] *See New Rules for Big Data: Regulators are Having to Rethink Their Brief*, ECONOMIST (Feb. 25, 2010), http://www.economist.com/node/15557487; *see also* Danah

the power of Big Data in my work on reidentification.[16] To the surprise of many, computer scientists have demonstrated that they can often take a database full of anonymized data—data in which things like names, social security numbers, and photos have been intentionally removed to protect privacy—and restore identity by studying patterns in the data.[17] Big Data will have a profound impact on privacy, one which is still being explored by legal scholars.[18]

Big Data promises to have the biggest impact of all on law enforcement. Soon, the third parties that already hold information about us will be able to infer private details about our lives, even things we intentionally withhold from them. Students in a class at M.I.T. claimed they could determine the sexual orientation of anonymous users based only on the patterns with which they friend others on Facebook.[19] Others have used off-the-shelf facial recognition software to connect photos taken on a cheap consumer web camera to user profiles on Facebook and a dating website.[20] Worse yet, they used the information they learned from Facebook to guess the first five digits of the person's social security number with reasonable success, building a simple pathway from a quick glimpse of a person in public to potential identity theft.[21]

This is just the beginning. As terrifying as these examples of Big Data seem to be, they still bear some connection to rational explanation. The worst will come when we throw rationality out the window and people begin to draw inferences that defy rational explanation and that reveal true facts about individuals that the

---

Boyd, *Privacy and Publicity in the Context of Big Data*, DANAH (Apr. 29, 2010), http://www.danah.org/papers/talks/2010/WWW2010.html.

[16] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

[17] *Id.* at 1703-04.

[18] *Id.*; Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011).

[19] Nadia Wynter, *'Gaydar' Project at MIT Attempts to Predict Sexuality Based on Facebook Profiles*, N.Y. DAILY NEWS, Sept. 22, 2009, at A1, *available at* http://articles.nydailynews.com/2009-09-22/entertainment/17932462_1_gay-sexuality-facebook ("Gay men had proportionally more gay friends than straight men, giving the computer program a way to infer a person's sexuality based on their friends.").

[20] Alessandro Acquisti et al., Presentation at BackHat 2011: Faces of Facebook: Privacy in the Age of Augmented Reality (Aug. 4, 2011), *available at* https://www.blackhat.com/docs/webcast/acquisti-face-BH-Webinar-2012-out.pdf.

[21] *Id.*

subjects may not even realize about themselves.[22] We are embarking on the age of the impossible-to-understand reason, when marketers will know which style of shoe to advertise to us online based on the type of fruit we most often eat for breakfast, or when the police know which group in a public park is most likely to do mischief based on the way they do their hair or how far from one another they walk.

E. The Surveillance Society

These four trends, taken together, enable the rise of a powerful, new surveillance society, one which raises significant new threats to privacy. To understand more fully what I mean by a new surveillance society, consider what happens when you combine the four advances—the one device, the cloud, the social, and Big Data—to enable an application that has been often in the news lately: location tracking.[23]

Before we consider the way the police can track our location today, think about how they tracked location in the past with a tracking beeper, an expensive, complex device that federal agencies expended great amounts of money to develop. These devices had to be long-lived, small enough to hide, yet big enough to hold large batteries.[24] To install these devices, the police had to risk discovery by sneaking onto a private driveway or into a parking garage.

Today, the use of a tracking beeper seems to be an unnecessary law enforcement risk, because almost every one of us voluntarily carries a personal tracking beeper. When switched on, mobile phones periodically ping the airwaves, looking for cell towers in close proximity.[25] Cell phone providers track these registrations to help route calls and monitor the health of their networks. But through a technique known as trilateration, one can take the record of cell tower usage and locate a person with great accuracy, even with "a level of accuracy that can approach that of GPS."[26]

---

[22] *E.g.*, Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, Feb. 19, 2012, at MM30 (describing use by Target of data analytics to identify pregnant potential shoppers).

[23] *See* Janice Y. Tsai et al., *Location-Sharing Technologies: Privacy Risks and Controls*, 6 I/S: J.L. & POL'Y INFO. SOC'Y 119 (2010); Strandburg, *supra* note 9, at 631-33 (discussing location tracking and the Fourth Amendment).

[24] Kim Zetter, *Caught Spying on Student, FBI Demands GPS Tracker Back*, THREAT LEVEL—PRIVACY, CRIME AND SECURITY ONLINE, WIRED (Oct. 7, 2010, 10:13 PM), http://www.wired.com/threatlevel/2010/10/fbi-tracking-device/ (quoting an unnamed former FBI agent explaining that newer tracking devices are hardwired to the tracked car's battery, obviating the need for its own power source). In 2010, two different people discovered these devices strapped to their cars and shared them with the press. *Id.*; *FBI Tracking Device Teardown*, IFIXIT BLOG (May 9, 2011), http://www.ifixit.com/blog/blog/2011/05/09/fbi-tracking-device-teardown/.

And, thanks to the rise of the smartphone, the FBI's ability to track cell phones increases every year. These phones almost always include a GPS chip and a digital compass (to indicate the direction the user is facing) and come loaded with software packages that coax the user to reveal his location to third-party services.[27] Even three years ago, private companies rarely cared where its online users sat on the globe except at the level of granularity of the nation, state, or province.[28] Today, location-based services are widely deployed and spreading quickly. Services like Loopt[29] and Foursquare[30] try to overlay social networks atop the physical grid, creating a new sport of "checking-in" to stores and restaurants. This is all fueled by new advertising models, and many companies in Silicon Valley are racing to squeeze the untapped dollars available to those who can market locally, viewing Groupon's success in this space with envy.[31]

---

[25] Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES, Mar. 26, 2011, at A1, *available at* http://www.nytimes.com/2011/03/26/business/media/26privacy.html ("[W]e are already continually being tracked whether we volunteer to be or not.").

[26] *ECPA Reform and the Revolution in Location Based Techonologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 112th Cong. 1, 10 (2010) (testimony of Professor Matt Blaze), *available at* http://www.crypto.com/papers/blaze-judiciary-20100624.pdf. Professor Matt Blaze described "'network based' location techniques [that] can give the position of virtually every handset active in the network at all times." *Id.* at 6.

[27] Jordan Robertson, *Your Phone, Yourself: When is tracking too much?*, USA TODAY (Apr. 23, 2011, 10:39 PM), http://www.usatoday.com/tech/news/2011-04-23-smartphone-tracking.htm.

[28] *See generally* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006).

[29] LOOPT.COM, https://www.loopt.com/ (last visited Feb. 21, 2012).

[30] FOURSQUARE.COM, https://foursquare.com/ (last visited Feb. 21, 2012).

[31] James Surowiecki, *Groupon Clipping*, NEW YORKER (Dec. 20, 2010), http://www.newyorker.com/talk/financial/2010/12/20/101220ta_talk_surowiecki ("The market for local advertising, which is really the business Groupon is in, is huge (more than $130 billion a year) and still relatively untapped online."); *see also* Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J. (Dec. 17, 2010, 10:01

Of course, the disintegration of privacy to the commercial sector is an old trend that has been remarked upon for years. Even so, these four relatively new advances—the one device, the cloud, the social, and Big Data—mark an acceleration of the trend. We have turned a corner in the graph of power/invasiveness over time. Thanks to the increasing power of portable devices and their emphasis on location awareness, the rise of the cloud, and the power of Big Data, the power, extent, sophistication, and interrelatedness of private systems of surveillance are increasing at rates that suggest a difference in kind not just degree.

II. THE DIMINISHED FOURTH AMENDMENT

While some legal scholars have argued that we abandon the reasonable expectation of privacy test, and still others have anchored the Fourth Amendment in principles other than privacy, none of these scholars has considered the central question of this Article: what if we are headed for a world without privacy? This shift in focus gives a different, more urgent impetus to some of the prescriptions that others have offered, but it also gives rise to the need for new prescriptions.

In a world without privacy, a Fourth Amendment focused on privacy becomes nearly a dead letter. Today's Fourth Amendment has been built around the reasonable expectation of privacy test, but no expectation of privacy will be deemed reasonable in a world without privacy. Even worse, the great bulwark of the Fourth Amendment, probable cause and a warrant, will become much less important as pervasive monitoring and record collection will give the police probable cause most of the time.

The diminishment of the Fourth Amendment will change police behavior. Police agencies will begin to abdicate their traditional role as conductor of surveillance, because it will be eclipsed by the powerful new systems of private surveillance. The FBI and other law enforcement agencies will shift from being active producers of surveillance to passive consumers, essentially outsourcing all of their surveillance activities to private third parties, ones

---

PM), http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html ("[A]ds targeted by location bring in two to five times as much money as untargeted ads.").

who are not only ungoverned by the state action requirements of the Fourth Amendment, but also who have honed the ability to convince private citizens to agree to be watched.

It is likely, however, that courts will resist this change, refusing to accept a nugatory Fourth Amendment. To save the Fourth Amendment, they will transform it, abandoning the reasonable expectation of privacy test. To replace it, courts may turn to legal scholarship, which to date has failed to fully elaborate what should come next.

A. The End of Self-Help Policing

Before examining what the rise of the surveillance society means for the Fourth Amendment, consider what it means for the practicalities of policing. We should expect a major shift in the center of activity of crime fighting from the police to private industry. The surveillance society will greatly diminish the importance of self-help policing.

In constitutional criminal procedure, the difference between self-help policing and assisted policing has received little attention, because almost all court attention has focused on the former. In the near century since *Olmstead*,[32] almost all of the cases discussing what new technology means for the Fourth Amendment have involved police self-help and home-grown tools. The police inserted the wires into the telephone lines in *Olmstead*,[33] mounted the recording device in *Katz*,[34] deployed its own microphones in *Goldman*[35] and *Silverman*,[36] chartered aircraft for their own use in *Ciraolo*[37] and *Dow Chemical*,[38] and installed their own tracking beepers in *Karo*[39] and *Knotts*.[40] Future students of the amendment are likely to marvel at these historical relics, trying to imagine a time when the FBI was forced to build its own tools and collect its own data. It will likely seem a far cry from the FBI they know: agents sitting in offices, acting as a central clearing house for the observations of private industry, mining their way through mountains of data collected by other people and for other purposes.

---

[32] Olmstead v. United States, 277 U.S. 438 (1928).

[33] *Id.* at 457.

[34] Katz v. United States, 389 U.S. 347, 348 (1967).

[35] Goldman v. United States, 316 U.S. 129, 131 (1942).

[36] Silverman v. United States, 365 U.S. 505, 506 (1961).

[37] California v. Ciraolo, 476 U.S. 207, 209 (1986).

[38] Dow Chem. Co. v. United States, 476 U.S. 227, 229 (1986).

[39] United States v. Karo, 468 U.S. 705, 708 (1984).

[40] United States v. Knotts, 460 U.S. 276, 277 (1983).

It is as if today's FBI has developed a sophisticated surveillance research-and-development arm with field offices named Apple, Google, Facebook, Comcast, and AT&T.[41] On the surface, these private labs seem similar to FBI labs with big buildings and smart engineers. But peel back a layer and it is obvious these labs can do something important that no FBI lab could ever hope to do—convince the surveillance targets of the world to consensually adopt their surveillance technologies, acting as a neat end-around circumventing the Fourth Amendment.[42]

Although few scholars have noted what the end of self-help policing means for the Fourth Amendment, some have noted the descriptive shift in the amount the police and intelligence community rely on the fruits of private surveillance. Jon Michaels has carefully tracked the increasing reliance on technological advances and private surveillance by the intelligence community.[43] Others have noted how much the CIA, FBI, and Defense Department rely on the services of data aggregators like ChoicePoint.[44]

As proof of the shift away from a self-help police force, consider the annual Wiretap Report. By statute, the Administrative Office of the United States Courts is charged with issuing a report each year that tallies the number of applications for court-ordered wiretaps in state and federal court and requires a small number of summary statistics about each jurisdiction.[45]

---

[41] *See* David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1177 (1999) (discussing "out-contracting, in which government agencies hire private security companies to perform work previously carried out by law enforcement officers," at the time, a rapidly growing practice).

[42] *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 908 (2008) ("People simply do not interface with the government in the same ways or with the same frequency as they do with the private sector, and thus the intelligence agencies find themselves particularly drawn to, and in some respects dependent upon, private data resources.").

[43] *Id.* at 901-66.

[44] Joshua L. Simmons, Note, *Buying You: The Government's Use of Fourth-Parties to Launder Data about "The People,"* 2009 COLUM. BUS. L. REV. 950, 994 (2009).

[45] 18 U.S.C. § 2519 (2006).

One table of the report breaks down wiretap orders by the "type of surveillance used," oral (voice), wire (telephone), electronic (computer network).[46] Some have expressed surprise, even suspicion, at the low number of electronic orders granted every year. For example, in calendar year 2010, out of 2,311 wiretaps ordered nationwide, only sixteen involved electronic surveillance (defined as "Digital Pager, Fax, and Computer"), or approximately 0.7%.[47] This is not an outlier, as indicated by Figure 1, which plots both the total number and percentage of all wiretaps that involved electronic surveillance for the past fifteen years.

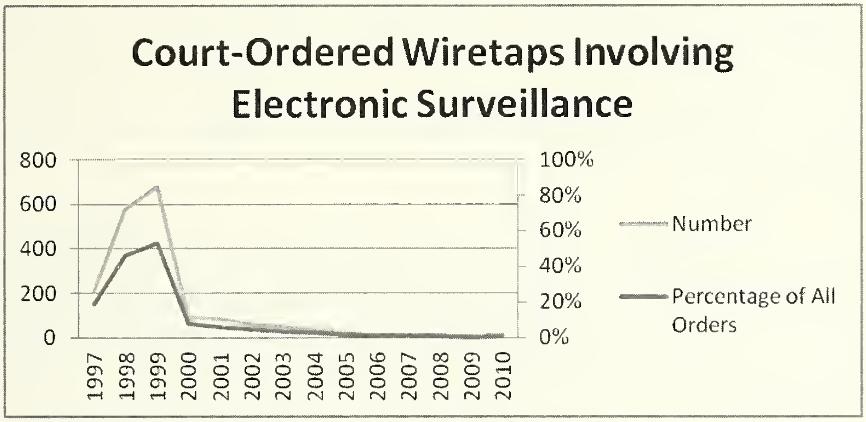


Figure 1: Court-Ordered Wiretaps Involving Digital Evidence (1997-2010)[48]

Figure 1 provides a compelling visual image of the decline of self-help policing. Clearly, the number of court ordered wiretaps involving electronic evidence dropped precipitously at the turn of the century. Chris Soghoian, a close watcher of these statistics, speculates that this is proof of the declining importance of fax transmissions in criminal surveillance, which are included in this reporting category.[49] But the drop since 2000 is nearly as pronounced, with a near linear decline from 2000 (eighty-nine intercepts, nearly eight percent of all)[50] to 2006 (thirteen intercepts, 0.76%).[51] Since 2006, the nation's courts have authorized fewer than twenty wiretaps of digital networks a year, never topping one percent of all orders in that time span.[52]

---

[46] *See, e.g.*, DIR. OF THE ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 27 tbl.6 (June 2011), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2010/Table6.pdf.

[47] *Id.*

[48] Figure 1 was constructed using data from the 1997 through 2010 *Wiretap Reports* issued by the Director of the Administrative Office of the United States Courts. For the detailed data see *Wiretap Reports*, UNITED STATES COURTS, http://www.uscourts.gov/Statistics/WiretapReports.aspx (follow "Wiretap Report YEAR" hyperlink for each yearly report; then follow "Table 6" hyperlink) (last visited Feb. 21, 2012).

The dramatic decrease is almost certainly not an indication that criminals use computer networks less or that the police rely less on network surveillance. Instead, it likely represents a shift in police tactics away from self-help. Today, it makes little sense for the police to engage in court-ordered wiretapping. Not only is it easier to secure private cooperation than judicial sanction, but also the fruits of private surveillance are simply better—fed as they are by our sensor-laden world and empowered by consensual sharing.

---

[49] Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, SLIGHT PARANOIA BLOG (Dec. 1, 2009, 7:00 AM), http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html ("I suspect that the nearly 700 electronic intercept orders granted in 1998 were largely for fax machines and pagers. Thus, as these technologies died out, it is only natural that the number of electronic intercept orders declined[.]").

[50] DIR. OF THE ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 27 tbl.6 (Apr. 2001), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2000/table600.pdf.

[51] DIR. OF THE ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 27 tbl.6 (Apr. 2007), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2006/Table62006.pdf.

[52] The Wiretap Reports indicate also the number of "Combination" wiretaps, which "refers to installed intercepts for which more than one type of surveillance was used." DIR. OF THE ADMIN. OFFICE OF THE U.S. COURTS, *supra* note 46. Since there are only three types of surveillance that might be joined in combination—oral, wire, and electronic—the odds are that some of the combination wiretaps involve electronic surveillance. Even if we assume that all combination wiretaps involve electronic surveillance—an unlikely possibility—the addition of these numbers does not change the trend substantially. To take one representative year, in 2008, out of 1809 wiretaps, ten were classified as involving electronic surveillance and thirty-three were combination, increasing the percentage from 0.55% to 2.38% of all wiretaps. DIR. OF THE ADMIN. OFFICE OF THE U.S. COURTS, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 27 tbl.6 (Apr. 2009), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2008/Table6.pdf

Figure 1 is a bellwether not an outlier. With each passing year, the police will learn to borrow and beg rather than build. Our mental image of the FBI agent conducting surveillance, wearing headphones in a white van parked on the curb, clipping alligator clips to telephone wires, and working with a white-coated FBI scientist will soon be replaced by an agent sitting in his office, hitting the refresh button on his web browser, and reading the latest log file dump sent from private industry.

Consider one final example. In the late 1990s, the FBI faced a firestorm surrounding its Carnivore system—a piece of software developed in-house and designed to perform electronic wiretapping on digital networks—in technical terms, a filtering packet sniffer.[53] The public story is well known: the press dug deep, the public complained, and Congress raged, ultimately passing laws requiring better reporting about the FBI's use of the system.[54] The less-well-known denouement is also telling: a few years after the controversy, the FBI abandoned Carnivore's successor, realizing that the private computer security industry had designed better filtering packet sniffers than the FBI could do on its own.[55] This shift is a herald of the shift in role and responsibility for surveillance from FBI labs to private companies, which we will see repeated constantly in the years to come.

B. No More Expectations of Privacy

In *Katz*, the Supreme Court embraced a new doctrine of the Fourth Amendment built on privacy. This took the form of the majority's pronouncement that "the Fourth Amendment protects people, not places,"[56] and Justice Harlan's "reasonable expectation of privacy" test in a concurring opinion,[57] which was later embraced by the Court as the test for the meaning of search within the amendment.[58] Although the rest of this Part will examine in-depth what happens to a privacy-centric Fourth Amendment in a world without privacy, the punch line is both easy to state and preordained almost to the point of being tautological—in a world without privacy, a Fourth Amendment built around reasonable expectations of privacy will no longer apply.

---

[53] Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 648-54 (2003).

[54] *Id.* at 654-58.

[55] Ted Bridis, *FBI Abandons its Software for Online Wiretaps, Bureau Switching to Commercial Snooping System*, CHI. TRIB., Jan. 19, 2005, at 12.

[56] Katz v. United States, 389 U.S. 347, 351 (1967).

[57] *Id.* at 360-61 (Harlan, J., concurring).

Specifically, the courts have given the reasonable expectation of privacy test three additional elaborations, and each suggests that when courts face fact patterns arising from the rise of the surveillance society, they might hold that the Fourth Amendment does not apply.

1. Assumption of Risk

According to the Supreme Court, an individual

> takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . [E]ven if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[59]

This reasoning has been applied in at least two important and broad contexts, which are both implicated by the surveillance society: the false friends rule and the third-party doctrine. Under the false friends rule, exemplified by cases like *Hoffa v. United States*,[60] we share secrets with other people at our own risk, and if the people we think are trusted confidants turn out instead to be government agents wearing a wire, we have only ourselves to blame, and the Constitution provides no relief.[61]

The reasoning has extended not only to friends but also to the companies we use for essential services. The Supreme Court has declared that the Fourth Amendment does not apply to our bank's records of our financial transactions,[62] or to our phone company's lists of numbers we have dialed.[63]

---

[58] Smith v. Maryland, 442 U.S. 735, 740 (1979).

[59] United States v. Miller, 425 U.S. 435, 443 (1976).

[60] 385 U.S. 293 (1966).

[61] *Id.* at 302.

Notice how this rule automatically expands police power to some of the new forms of private surveillance. Consider for example the location records people now share regularly with Loopt[64] and Foursquare.[65] Because we share our location consensually with companies like these, courts are likely to treat this information as constitutionally unprotected under the reasoning of the assumption of risk cases.

2. Knowing Exposure

Under the knowing exposure rule, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[66] The Supreme Court has used this reasoning to rule that the police can track a car with an electronic beeper as it moves around city streets, because the car remains on public thoroughfares.[67] It has also used the concept of knowing exposure to deem outside the Fourth Amendment the use by the police of airplanes and helicopters to look at the open fields and even the curtilage next to a person's home.[68]

Knowing exposure means that some of the information shared online through private services may be accessed by the police, because new online services obscure the already blurry line between what we treat as private and public. Consider for example what you say on your Facebook account. Is a Facebook account a public or private space? Does it depend on the number of friends you have or the configuration of your privacy settings? Complicating this considerably is Facebook's ongoing war with its users about those privacy settings and, in particular, what the default settings should be. A court could reasonably hold that some of the content posted to Facebook has been knowingly exposed to the public and, following conventional Fourth Amendment law, rule that it may be obtained by the police without a warrant.

---

[62] *Miller*, 425 U.S. at 442-43.

[63] *Smith*, 442 U.S. at 744-45.

[64] LOOPT.COM, *supra* note 29.

[65] FOURSQUARE.COM, *supra* note 30.

[66] Katz v. United States, 389 U.S. 347, 351 (1967).

[67] United States v. Knotts, 460 U.S. 276, 282 (1983).

[68] Dow Chem. Co. v. United States, 476 U.S. 227, 238-39 (1986); California v. Ciraolo, 476 U.S. 207, 214-15 (1986).

3. General Public Use

Finally, the general public use rule comes from two cases, *Dow Chemical*[69] and *Kyllo*.[70] According to this rule, the police may deploy powerful surveillance devices to track suspects without a warrant so long as the tool is generally accessible to the public. In *Dow Chemical*, the court held that a $22,000 camera qualified under this rule.[71] Although the Court backtracked a bit in *Kyllo*, finding a $1000 thermal heat-imaging machine did not qualify as one in general public use, it refused to overrule *Dow Chemical*.[72]

As the power of private surveillance increases, the devices and systems they create may be available to the police without process because of this rule. Consider for example powerful reidentification techniques. Some day, private companies may develop a tool to convert the supposedly anonymous comments on a public message board into the commenter's true identity by cross-referencing the attributes of the communication with rich outside databases using powerful reidentification techniques.[73] Whether the police could use technology like this without a warrant may turn on the general public use test, which means a warrant may not be needed once reidentification tools become cheap and widespread.

Because of these three rules, the systems of private surveillance I sketched in Part I may become, by default and in lockstep, a system of public surveillance. The coming surveillance system could give rise to a powerful, pervasive surveillance state, at least if traditional approaches to the Fourth Amendment apply. With each passing year, the police might find that their power grows with every industry product launch. The people would be watched in ways that they would not have been; records of their behavior would be created and retained when once they would have been never created or destroyed; and traditional forms of surveillance would occur much more thoroughly and efficiently than they have before.

---

[69] 476 U.S. at 227.

[70] Kyllo v. United States, 533 U.S. 27 (2001).

[71] 476 U.S. at 238.

[72] *Kyllo*, 533 U.S. at 39 n.6.

[73] *Cf.* Farkhund Iqbal et al., *A Novel Approach of Mining Write-Prints for Authorship Attribution in E-Mail Forensics*, 5 DIGITAL INVESTIGATION 42-51 (2008), *available at* http://www.dfrws.org/2008/proceedings/p42-iqbal.pdf (describing statistical techniques that can identify authors of anonymous writings).

C. The Inevitable Search for the New Fourth Amendment

It is possible that courts will follow the doctrinal path sketched above, issuing a series of opinions that render the Fourth Amendment a dead letter. Perhaps the Fourth Amendment will fade into the dustbin of history, following the Third Amendment's right against state mandated quartering of soldiers as another idea that galvanized the founding generation but one that speaks to outmoded fears and superseded values. Future courts might reason that as privacy fades, because the citizenry forfeits more and more sensitive information to the private sphere, it takes with it the need for this particular constitutional protection. They might see changing social norms spurred by shifting technological possibilities as a fundamental shift in the foundation upon which the original Framers built, a reason to redefine reasonableness, search, and seizure.

But it seems unlikely that courts will take this particular path. Courts seem unlikely to abandon one of the principle limitations of state power in our founding document, an amendment that Akhil Amar argues "literally and in every other way, belongs at the center of the Bill of Rights."[74] This is true regardless of the political priors of judges considering the question and the method of constitutional interpretation he or she embraces. Originalists and textualists will argue that the amendment was never really about privacy at all. Living constitutionalists will find within the open texture of the amendment's language the freedom to shape the concept of unreasonable search and seizure to changed circumstances.

The result will be a concerted effort to find new underpinnings for a new interpretative theory and jurisprudence of the Fourth Amendment. Unfortunately, the judges engaged in this effort will find very little concrete guidance in legal scholarship, because even though many scholars have grumbled about the amendment's shortcomings, the answers they have offered are inchoate, only partially defined, and ultimately not nearly enough to provide a way forward.

---

[74] Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 811 (1994).

D. Other Solutions and Their Limits

Today, few legal scholars speak in favor of *Katz* and the reasonable expectation of privacy test, and even fewer can muster anything kind to say about the third-party doctrine.[75] One would expect, therefore, to find answers in the prescriptive approaches that they have presented. Although some of these scholars have discovered useful frameworks pointing to what comes next, none has yet come close to offering the judges who will soon abandon reasonable expectations of privacy a detailed and concrete way forward.

Some authors have proposed abandoning the third-party doctrine.[76] Others have advocated a redefined Fourth Amendment that focuses on power instead of privacy.[77] Still others have recommended viewing the Fourth Amendment as a question of policy rather than mere expectations.[78] These writers offer useful starting points, but none comes close to offering a fully realized theory. Some offer abstract prescriptions that are too difficult to translate into useful, predictable rules. Others offer solutions that are more concrete but unfortunately do not go far enough to restoring a meaningful role for the Fourth Amendment.

One reason why none of these authors has gone far enough may be because none has been willing to follow the conceit of this Article—that privacy may soon vanish from this country. These authors have all recognized, to greater or lesser extent, that privacy is on the decline or has rapidly been redefined, but these middle-strength observations and predictions have given rise to proportionate half measures. But if privacy is almost a dead letter, and if the end of it will come soon, then the limits of these past prescriptions are clear.

---

[75] *But see* Kerr, *supra* note 3 (offering a defense of the third-party doctrine).

[76] *See infra* Part II.D.1.

[77] *See infra* Part II.D.3.

[78] *See infra* Part II.D.2.

1. Why Abandoning the Third-Party Doctrine Isn't Enough

The standard move made by legal scholars in articles like this is to focus on the third-party doctrine—the rule that states:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[79]

Or, more concisely, "[b]y disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed."[80]

Some critics contend that the third-party rule is a mistake in every context and should be overturned.[81] Others would restrict it to its original contexts—bank records and telephone numbers dialed—but prevent it from spreading to other network services like electronic mail, cloud computing, and mobile location.[82] What remains consistent throughout this literature is the idea that the third-party doctrine deserves to be our central focus, that if only we could rein it in, we could right the balance between police power and privacy. Fixing the third-party doctrine, in short, is both necessary and sufficient to fixing the problem of police surveillance of private behavior.

In a world without privacy, however, getting rid of the third-party doctrine is necessary but not nearly sufficient to ensure the appropriate protection of the Fourth Amendment. The third-party doctrine and, more broadly, the Fourth Amendment have traditionally evolved to focus attention almost entirely on the requirement that a search warrant be issued only with probable cause and particularity.

---

[79] United States v. Miller, 425 U.S. 435, 443 (1976).

[80] Kerr, *supra* note 3, at 563.

[81] Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 265 (2006).

[82] Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1407 (2004) ("[T]he argument that, under *Miller*, the mere fact that a subscriber places his or her communications with a third-party service provider eliminates any expectation of privacy in those communications is doctrinally and normatively unsound."); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 41, *available at* http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf ("The analogy between banking records and stored e-mails does not hold."); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1578 (2004).

In a world without privacy, probable cause and a warrant by themselves will not do enough to give effect to the full protection of the amendment. Although judges will be able to squelch fishing expeditions, fishing expeditions will no longer be necessary.[83] This is the power of a widespread surveillance society. It produces interconnected databases that track the behavior of millions in excruciating detail, gives companies (and the police agencies they assist) detailed records of what every one has done, and produces chains of evidence that can connect criminals to crime with no breaks and no ambiguous midway points.[84]

The result is that even if we increase probable cause and warrant requirements, we still will be subject to far too much arbitrary surveillance. If the police are tracking a person knowing only the time and place of the crime and a general description of the perpetrator, they will be able to access cell phone location databases or video surveillance log files (with probable cause) to make the match. If they know that a particular e-mail address was used, then they will be able to search the login databases for the e-mail provider.

Reversing or narrowing the third-party doctrine will help stem official arbitrariness, but it will not do enough to reverse the unprecedented increase in police power that the surveillance society has created. The problem with the surveillance society is not simply how it empowers the bored police officer on a fishing expedition; it is a broader problem with an increase in the power of the state to watch, listen, and follow every one of us.

2. The Limits of Policy

Many scholars dissatisfied with the evolution of the reasonable expectation of privacy test since *Katz* recommend that judges replace it or implement it using a first-principles, free-wheeling, normative style of analysis. They take as both their inspirational model and precedential green light Justice Harlan, who not only invented the reasonable expectation of privacy test in his *Katz* concurrence, but also shortly thereafter tried (in dissent) to modify it to embrace this kind of naked, normative mode of analysis.[85] Justice Harlan argued:

---

[83] Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514, 1544 (2010).

[84] *Id.* at 1530-32. *See also infra* Part III.D.

> Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society. The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens, the risks of the electronic listener or observer without at least the protection of a warrant requirement.[86]

Justice Harlan explained further that he was proposing a balancing test of "assessing the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement."[87]

As we search for a replacement for reasonable expectation of privacy, Justice Harlan provides a potential starting point, but not more than that. The problem with the purely normative inquiry is its imprecision and variability. A test that explores solely "the desirability of saddling [particular practices] upon society"[88] is a non-test, which invites little more than rules based on the prior predilections of each judge. Even worse, such a starting point will lead to complete unpredictability, at least to start, which will leave police officers incapable of knowing what to do in most situations, particularly those involving new, untested waters. Given the severe sanction of the exclusionary rule, this kind of uncertainty is unacceptable.[89]

---

[85] *See, e.g.*, Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *is Made Of?*, 41 U.C. DAVIS L. REV. 781, 795 (2008) (discussing the "'is-ought' problem" of the reasonable requirement); Catherine Hancock, *Warrants for Wearing a Wire: Fourth Amendment Privacy and Justice Harlan's Dissent in* United States v. White, 79 MISS. L.J. 35, 35 (2009); Freiwald, *supra* note 82, ¶¶ 30-31 (discussing the need for a "normative inquiry").

[86] United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

[87] *Id.*

[88] *Id.*

The other reason to be wary of a pure policy interpretation of the Fourth Amendment is the tendency for policy debates about privacy and security to end up one-sided. In his book, *Nothing to Hide*, Daniel Solove catalogs a number of distorting features of the debate between privacy and security that tend to push decision makers to privilege security.[90] For example, he discusses the common retort that privacy is needed only for those with something embarrassing or shameful they want to conceal—the nothing-to-hide argument[91]—or the fallacy that privacy and security are inversely proportional qualities locked in a zero-sum tournament—the all-or-nothing belief.[92]

3. From Privacy to Power

If the Fourth Amendment does not intrinsically promise privacy, what does it provide? Many scholars have argued that the Fourth Amendment should be interpreted as being about power, not just privacy. Some place this in an originalist frame. The colonists designed the amendment to respond to the Crown's use of general warrants, blanket authorities that entitled British troops to search people and homes (and "papers and effects") indiscriminately and without suspicion.[93] Although these indignities involved privacy harms, the more important problem seemed to be the way they defined their relationship with the state, a relationship marked by insecurity and imbalanced power.

Now that privacy is fading, we need to take the claims of these scholars more seriously if the Fourth Amendment is to survive. The end of privacy disrupts the rules we use to give action to the amendment, and we must shift away from *Katz*'s reasonable expectation of privacy to rules that focus instead on the balance of power between the police and the people.

---

[89] Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 527 (2007) ("The Fourth Amendment's suppression remedy . . . generates tremendous pressure on the courts to implement the Fourth Amendment using clear ex ante rules rather than vague ex post standards.").

[90] DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011).

[91] *Id.* at 21-32.

[92] *Id.* at 33-37.

[93] Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 296-97 (1993).

In his book, *Nothing to Hide*, Dan Solove recommends that we abandon the reasonable expectation of privacy test, because it is "not focused on the right question."[94] This is because "[i]n many instances, what is or isn't protected by the Fourth Amendment bears no relation to the problems caused by government information gathering"—namely, "whether it is best to have judicial oversight of law enforcement activity, what that oversight should consist of, how much limitation we want to impose on various government activities, and how we should guard against abuses of power."[95]

Law professor Thomas Clancy has sounded a similar theme in urging courts and legal scholars to conceptualize the Fourth Amendment as not only about privacy and property but also "security from unreasonable governmental intrusion."[96] This interpretation of the amendment, which of course finds better textual support than "privacy,"[97] stemmed from the colonists' experience with the "arbitrary exercise of [British] power to invade their property."[98] "The Framers valued security and intimately associated it with the ability to exclude the government."[99] In similar terms, Jed Rubenfeld has argued that "[t]he Fourth Amendment does not guarantee a right of privacy. It guarantees—if its actual words mean anything—a right of *security*."[100]

Other scholars have made similar points. Morgan Cloud has argued that "[t]he text and history of the Fourth Amendment demonstrate that it exists to enhance individual liberty by constraining government power."[101] Bill Stuntz argued that the

---

[94] SOLOVE, *supra* note 90, at 114.

[95] *Id.* at 115.

[96] Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 351 (1998) (internal quotation marks omitted).

[97] *See* U.S. CONST. amend. IV ("The right of the people to be *secure* in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated" (emphasis added)).

[98] Clancy, *supra* note 96, at 352.

[99] Clancy, *supra* note 96, at 353.

[100] Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 104 (2008).

[101] Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 618-19 (1996); *see*

Fourth Amendment should focus not only on privacy, but also on "concern with coercion and violence."[102] Thomas Crocker finds that the Fourth Amendment does not adapt well to new forms of "social privacy," suggesting instead that it "should be refocused in light of the protections provided interpersonal liberty."[103]

III. THE FOURTH AMENDMENT'S THIRD ACT

A. Katz *is the New* Olmstead

In one hundred years, when we look back on the history of the Fourth Amendment, we will realize that for a long time we misunderstood the relationship between privacy and the amendment. We think of them today as intrinsically connected, but this is an illusion.

Privacy is simply a proxy for what the amendment protects. It is a proxy that served us well for a long time because technology and social practices have historically moved so slowly. But today, nothing seems to move as quickly as technology, and nothing in the text of the amendment explicitly depends on privacy or on a society that respects privacy. This may seem surprising, both because the Fourth Amendment has for so many decades focused on privacy, but also as a matter of textual analysis. The amendment's central focus on the word "search" suggests a natural connection to the concept of privacy.

But the age of using privacy as a measuring stick for Fourth Amendment protection is likely soon to draw to a close. Of course, a similarly radical shift has happened before. The earliest cases conceived of the Fourth Amendment as designed to protect property, with this view reaching its zenith in the *Olmstead* Court's refusal to extend the amendment to wiretapping because "[t]he language of the Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of

---

also Cloud, *supra* note 93, at 295 ("The fourth amendment exists for the very purpose of enhancing individual liberty by constraining government power.").

[102] William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 446 (1995).

[103] Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After* Lawrence, 57 UCLA L. REV. 1, 56 (2009).

his house or office any more than are the highways along which they are stretched."[104] Almost four decades later, this style of reasoning was entirely repudiated, and the foundation of the Fourth Amendment was swapped out completely, replaced by the reasonable expectation of privacy test.[105] The Fourth Amendment survived one fundamental shift; it is due for another.

And when the history of our current epoch—the Fourth Amendment's second act—is written, we will probably consider it a happy accident that our conceptions of privacy and power served one another so well for so long. As Thomas Crocker puts it:

> Fourth Amendment privacy and the liberty ordinarily protected under due process may overlap, and the former may be valued for its ability to foster the latter, but the two need not always coincide. Thus, if the Fourth Amendment is understood to protect liberty as well as privacy, new constitutional possibilities emerge for shielding interpersonal relations from state intrusion.[106]

Privacy, with all of its messy connotations and contextual variation, has seemed to map, more or less appropriately, with the balance of power we wanted vis-à-vis the state. It does no more, and we need to start over, again.

We will be eased in our task of abandoning the fundamental underpinning of the Fourth Amendment by learning lessons from the last time we did something similar. The most important lesson we can learn is that though today we look past property in elaborating the Fourth Amendment, we have never really abandoned it. Contrary to Justice Stewart's admonishment that the "Fourth Amendment protects people, not places,"[107] today's Fourth Amendment rules continue to treat different places in different ways.[108] Privacy has given us new protections in new contexts, but property still remains.[109] Similarly, as we transition to a Fourth Amendment based on power not privacy, we should expect to continue to talk and think about privacy for many years.

---

[104] Olmstead v. United States, 277 U.S. 438, 465 (1928).

[105] *See* Katz v. United States, 389 U.S. 347 (1967).

[106] Crocker, *supra* note 103, at 59.

[107] *Katz*, 389 U.S. at 351.

[108] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809 (2004) ("[T]he basic contours of modern Fourth Amendment doctrine are largely keyed to property law.").

Moreover, what property and privacy have in common is that they were both imperfect proxies for what the amendment actually protects. Until the advent of the telephone, property served as a bright-line proxy for the border between state scrutiny and private action. With the rise of the telephone, airplanes, and heat-sensing devices, privacy stood as an imperfect, but still reasonable, proxy for drawing that same borderline.

With the rise of widespread intermediation, portable sensing, and content storage, privacy is no longer serving as an appropriate proxy. The new constitutional lodestar, power, is the Fourth Amendment's third act. There is reason to believe, however, that this might be the final act. Power seems to be the amendment's essence, not merely a proxy for something deeper. If power (and liberty) is not the core of the amendment, it is close to being so, much closer than anything we have used before.

B. Private Power and State Action

In the coming world, when the police outsource surveillance to private third parties, a revised Fourth Amendment focused on maintaining a constitutional balance of power should cast much more scrutiny than it does today on how the private choices of private actors can disrupt this balance of power. But constitutional jurisprudence, built firmly atop a foundation of state action, does not lend itself easily to the idea that private action can give rise to constitutional problems.[110] This seemingly fundamental barrier to the development of a new foundation for the Fourth Amendment misses an important point. With the rise of the surveillance society and the concomitant decline of police self-help, although the police will no longer be collecting information in the initial instance, they will still need to request the information from some third party, an unambiguous state action.

---

[109] Shortly before the final editing stages of this Article, the Supreme Court decided the landmark GPS-tracking case, *United States v. Jones*, 132 S. Ct. 945 (2012). The majority opinion by Justice Scalia embraces a decidedly property-centric view of the Fourth Amendment. *Id.* at 949.

[110] This is similar to, but ultimately different from, the welcome attention David Sklansky has paid to the private police. *See* Sklansky, *supra* note 41. Sklansky's discussion of the legal implications of the private police involves a rich account of the state action doctrine as it has been applied to criminal procedure, a topic that "has been largely neglected both by constitutional scholars and by criminal procedure scholars." *Id.* at 1230.

In the future, the police request alone will satisfy state action. This form of state action will seem different from the kind we witness today in two seemingly important ways that courts should acknowledge without getting too bogged down. First, the "action" of the state will seem thin compared to the cases we think about today. The police will not be climbing telephone poles or running packet sniffers, but instead will receive DVD-ROMs by messenger. Second, although tomorrow's state-action requirement will be met by little more than a simple police request, this should not bar a jurisprudence of Fourth Amendment "reasonableness" that focuses on the contents and structure of databases held by private parties, which means that the constitutionality of a search under the Fourth Amendment might depend on what happened during the time before state action. The decision of reasonableness might turn, for example, on why a private company has, say, a database tracking the location of private citizens to begin with, which will lead to a constitutional decision that will turn on pre-state-action facts.

C. Equilibrium Adjustment and the Surveillance State

How then does a Fourth Amendment designed to limit undue government power operate? What takes the place of the venerable reasonable expectation of privacy test, and do we preserve the historically important role of the warrant and probable cause requirements?

1. The Equilibrium-Adjustment Theory

In his recent article, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, Professor Orin Kerr identifies an underappreciated but, to his mind, near-universal goal driving how the courts have interpreted the Fourth Amendment in the face of technological change: balance[111] Kerr argues:

---

[111] Kerr, *supra* note 4.

> When changing technology or social practice makes evidence substantially harder for the government to obtain, the Supreme Court generally adopts lower Fourth Amendment protections for these new circumstances to help restore the status quo ante level of government power. On the other hand, when changing technology or social practice makes evidence substantially easier for the government to obtain, the Supreme Court often embraces higher protections to help restore the prior level of privacy protection. Fourth Amendment protection resembles the work of drivers trying to maintain constant speed over mountainous terrain. Judges add extra gas when facing an uphill climb and ease off the pedal on the downslopes.[112]

Kerr is adding rigor to several common intuitions about the Fourth Amendment: it should be technology-neutral and it should protect a level playing field.[113] Kerr argues that he has identified a theory that finds common ground among almost every Supreme Court Justice and interpretative theory that has ever tackled constitutional search and seizure. He argues that his "equilibrium-adjustment" theory can explain the approach of living constitutionalists, textualists, and originalists alike.[114]

Kerr is onto something. He identifies a pervasive and underappreciated thread running through the Fourth Amendment jurisprudence of technological change. I share his enthusiasm for this construct and his optimistic belief that we might be able to use it—properly fleshed out—to both rationalize some of the hard-to-theorize differences in doctrine as well as convince those who disagree about a given outcome that they are closer together than they appear.

Kerr's theory does a reasonably good job rationalizing past cases. For example, he convincingly explains how equilibrium adjustment can explain the "rather strange line" that regulates the use of tracking beepers by the police—no warrant needed on city streets but warrant needed inside the home[115]—as the Court's attempt to draw lines to try to maintain balance in the face of technological change.[116] He likewise does a nice job bringing a bit of coherence and rigor to the automobile cases, which hold that people enjoy fewer Fourth Amendment protections in cars than in other contexts, a notable accomplishment given how the judges themselves tend to provide only thin justifications.[117] Whereas these judges offer platitudes about how the mobility of automobiles can thwart crime fighting, or hopelessly circular arguments about how we expect less privacy in vehicles that are so often stopped without a warrant,[118] Kerr argues that the exception has stemmed mostly from equilibrium adjustment, and from attempts to level the playing field.[119]

---

[112] *Id.* at 480.

[113] *Id.*

[114] *Id.* at 526-27.

[115] *See* United States v. Karo, 468 U.S. 705, 714-15 (1984); United States v. Knotts, 460 U.S. 276, 282 (1983). Kerr wrote his article before the Supreme Court revisited

But these two examples share one important feature in common—they each involve a technology that benefits only one side of the crime-fighting equation: the police (tracking beepers) or the criminals (automobiles). Kerr's theory, at least as he explicates it, performs not nearly as well when applied to new technologies used by "both criminals and the police."[120] Notably, most of the technologies in this problematic category tend to be the very same technologies that are the focus of this Article, technologies developed by private parties for private purposes that generate records useful to the police.

2. The Problem with the Balance Sheet Approach

When faced with technologies that create avenues for both committing and detecting crime, the problem for equilibrium adjustment is trying to figure out how to account for which direction and by how much the level playing field has shifted. The advent of the telephone made the life of a criminal both easier and more difficult. The theory of equilibrium adjustment requires us to determine which of these two impacts outweighs the other.

---

tracking beepers in *United States v. Jones*, 132 S. Ct. 945 (2012), decided shortly before this Article entered its final editing stage.

[116] Kerr, *supra* note 4, at 499-501.

[117] *Id.* at 502-08.

[118] *E.g.,* California v. Carney, 471 U.S. 386, 392 (1985) (explaining that automobiles deserve a "reduced expectation of privacy" because they are so often searched without a warrant).

[119] Kerr, *supra* note 4, at 507-08.

[120] *Id.* at 489.

Kerr tackles this problem using an informal accounting.[121] A judge should "recreat[e] the same limits on surveillance over the telephone network that exist on equivalent surveillance in the physical world."[122] The judge must account for all of the upsides and downsides the telephone brought to crime and crime fighting by comparing the new balance of the playing field to the one that existed before the invention of the phone.[123] To answer this empirical question, Kerr seems to suggest that judges should make lists that summarize the technological pros and cons experienced by criminals or the police.[124] This is not precise and feels intuitive and squishy. It turns out to be a messy, imprecise undertaking.

Perhaps too conveniently, Kerr's informal accounting leads him to support precisely the mix of Fourth Amendment rules we have today. Telephone surveillance, Kerr argues, triggers the Fourth Amendment because "the contents of phone calls . . . played the modern-day role of private meetings that were protected" before the telephone.[125] "As a result, the power to monitor communications in a phone booth when a person placed a call was the modern equivalent to the power to break into a home and listen to conversations there."[126] With this part of the analysis, I agree.

Where I disagree with Kerr is in his treatment of non-voice surveillance of numbers dialed. Pen registers and trap and trace devices should not trigger the Fourth Amendment under equilibrium adjustment he concludes, because they help level the playing field in favor of the police to make up for the advantages felt by criminals.[127] "The telephone network," Kerr explains, "provides criminals a substitute for traveling out in public and then meeting with conspirators in private, and the *Katz/Smith* line maintains the equilibrium of privacy that existed with the physical meeting for the telephone equivalent."[128] For this proposition, he does not cite studies or specific cases; this is an exercise mostly in common sense intuition. Because the telephone has tilted the playing field too far in favor of criminals, Kerr concludes that, at least for pen register and trap and trace surveillance, the courts should create a rule weighted in favor of the police: the police should be allowed, without a warrant, to compile a list, in real time, of the circle of people a person communicates with on the phone in order to restore a power they used to have before the phone.[129]

---

[121] *Id.* at 512-17.

[122] *Id.* at 513.

[123] *Id.* at 512-17.

[124] *Id.*

[125] *Id.* at 515.

[126] *Id.*

[127] *Id.* at 516-17.

[128] *Id.* at 517.

Unfortunately, this informal accounting fills in only half of the balance sheet. The criminals are not the only ones who benefited from the rise of the telephone.[130] Telephone companies develop sophisticated systems of private surveillance that collect new pieces of information about communications (and, by simple extension, relationships and conduct) that once were never stored anywhere. Because these records—most importantly the record of calls made—get stored by default and retained for a long time, the police can recreate past behavior dating back before the target was even a target. The telephone, in other words, dramatically improves law enforcement's ability to conduct ex post investigations when compared to pre-telephone, physical world crimes. Crimes committed in the physical world, say stalking or the whispered conversations between co-conspirators, do not leave permanent records as a matter of course. In the pre-telephonic era, the police did not know where to look until the crime was detected and reported. The phone, in other words, has made crime fighting much easier.

---

[129] *Id.* ("Under *Smith*, the police can watch the network equivalent of public space to learn who the suspect called and when.").

[130] I am not the first to lodge this critique at Kerr. In response to an earlier, less-developed version of the argument, which Kerr called one of substitution effects, several commenters made similar points. *See, e.g.*, Erin Murphy, *The Case Against the Case For Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1244 (2009) ("[I]t seems probable that the more that third-parties are involved or technology is deployed, even with a robust conception of third-party protections, the more likely it becomes that the criminal will be apprehended. This is for the simple reason that enlisting third-party assistance in crime tends to generate, rather than obfuscate, opportunities to get caught. Third parties increase the possibility that a trail will be left or witnesses will be created, all of which only helps the state in building its case."); *see also* Blake Ellis Reid, Note, *Substitution Effects: A Problematic Justification for the Third-Party Doctrine of the Fourth Amendment*, 8 J. TELECOMM. & HIGH TECH. L. 613 (2010). "The neutrality argument, however, relies on the false premise that law enforcement has an *unlimited* capability to surveil low-tech public activities and a limited capability to surveil high-tech private activities. As discussed below—both generally and in the context of *Miller* and *Smith*—the opposite is often true." *Id.* at 620.

This problem is not specific to telephones. Kerr's balance sheet approach is hard to use with any new technology for many reasons. First, every technology is a moving target, so it is a daunting task to ask a judge to characterize it accurately at one frozen moment in time. Second, lawyers and judges quite often explain and understand technology using analogies and metaphors. But, analogical comparisons seem to be a poor tool for a judge trying to make the kind of accurate and detailed accounting Kerr proposes.[131]

Third, most complex technologies present multiple levels of generality, and it is not clear at which level of generality the court should focus. For example, assume a court had to apply Kerr's test not to the 1970's *Smith v. Maryland* telephone network, but instead to the 2012 telephone network. Weighing both pros and cons, do criminals experience a net benefit or burden from the shape and configuration of the modern phone network? The court faced with this question will face a dizzying array of levels of generality. The traditional circuit-switched network discussed in *Smith* was made less private, and thus less useful for criminals, with the introduction of Caller ID.[132] Then again, Caller ID can be disabled easily in most places.[133] Similarly, the privacy of a telephone line has been altered through the introduction of technologies like Signaling System 7, which separates control signals from the content of voice conversations and creates something like a structural "envelope" around phone calls.[134] Then again, laws like the Communications Assistance for Law Enforcement Act obligates telephone companies to ensure the easy wiretapability of digital phone switches. And we have not even considered the

---

[131] Professor Kerr himself has written about the perils judges face applying analogues for new technology. *See* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357 (2003).

[132] Glenn Chatmas Smith, *We've Got Your Number! (Is It Constitutional to Give It Out?): Caller Identification Technology and the Right to Informational Privacy*, 37 UCLA L. REV. 145, 149-50 (1989).

[133] *See* FCC Calling Party Telephone Number Privacy Rule, 47 C.F.R. § 64.1601 (2005) (mandating per-call blocking of Caller ID for interstate calls).

[134] *See* Jonathan Jacob Nadler, *Give Peace a Chance: FCC-State Relations After California III*, 47 FED. COMM. L.J. 457, 502 n.229 (1995).

Internet yet.[135] If you include VoIP, Skype, and Google Voice, the already murky becomes almost entirely inscrutable.[136]

Fourth, as we work our way down the back-and-forth, pro-and-con list making of the kind just demonstrated, we are never told by Kerr when to stop. Consider once again the pros and cons of the telephone. Telephones make it harder to catch harassers, Kerr reasons, by letting them stalk their victims from the comfort and privacy of the home.[137] But, on the other hand, as discussed above, crimes committed in the real world do not routinely leave detailed records behind, so the life of the police has been made easier. Unless, of course, we analogize stored phone records to how eyewitnesses in the real world get to see suspicious people driving around town just before the crime. But, on the other hand, eyewitnesses may not be nearly as reliable as the stored record of an incriminating phone call. This is what happens with the balance sheet approach: each side of the ledger will grow and grow, and we will be locked in a state of seemingly infinite regress.

Fifth, and finally, assume we find our way out of infinite regress. What then? We will be left with two impressively long lists. New technology has both made it easier to commit and to fight crime. What does this mean for the Fourth Amendment? The easiest conclusion is Kerr's: to assume that the pros and cons cancel each other out, leaving us with a tool that does little more than justify the rules we have today.[138] That seems too coincidental to be useful. For these five reasons, the balance sheet approach is not redeemable. We need another, more objective, and more rigorous way to measure the effect of a new technology on crime and crime fighting.

3. New Metrics for Equilibrium Adjustment

The answer is to ask the question much more directly, never losing sight of our new normative goal, the preservation of the balance of power between the citizens and the police. The ultimate question should be: How has technology altered the *metrics* of crime fighting? Are more people going to prison? Fewer? Are leads easier to develop today? Harder? How long does each investigative step take to accomplish? Here is an admittedly unorthodox proposal: it should take, on average, just as long to solve a crime today as it has in the past. Through the Fourth Amendment the Framers provided a fixed ratio between police efficiency and individual liberty, and as technological advances change this ratio, judges can interpret the amendment in ways to change it back.

---

[135] 47 U.S.C. §§ 1001-10 (2006).

[136] *See In re* Commc'ns Assistance for Law Enforcement Act and Broadband Access and Servs., 20 FCC Rcd. 14,989 (2005) (granting Justice Department petition to extend authority of CALEA to VoIP services).

[137] Kerr, *supra* note 3, at 578.

[138] Kerr, *supra* note 4, at 517 ("Taken together, *Katz* and *Smith* maintain the balance of power over the shift from physical surveillance to telephone surveillance.").

Some might react negatively to the idea that the Constitution mandates an inefficient constabulary, particularly in cases of ongoing victimization.[139] But throughout the history of Fourth Amendment jurisprudence the courts have enacted rules and holdings that force the police to be more inefficient in their duties than they would be without these rules and holdings. Every procedure imposed by the Fourth Amendment (and the Fifth and the Sixth, too) creates a more inefficient constabulary. Warrants take time to draft; subpoenas get met by motions to quash; and probable cause develops slowly. Until now, police efficiency standing alone has not amounted to unconstitutionality. If we reconceive of the Fourth Amendment as a regulator of power and liberty, not merely privacy, it is hard to see why the Constitution would prohibit such a construction.

A Fourth Amendment that forces police inefficiency might also be defended simply as a mirror image of the current Fourth Amendment, which often generates new rules designed to ensure criminal inefficiency. When criminals find a new tool of efficiency, such as the automobile, the Court will often decrease Fourth Amendment protections in order to rebalance the privacy/security balance that is supposedly at the heart of the reasonable expectation of privacy test.[140] Under current Fourth Amendment jurisprudence, insecurity justifies creating artificial criminal inefficiency; under the new Fourth Amendment jurisprudence, excessive government power will justify creating artificial police inefficiency.

---

[139] In fact, the Supreme Court has said as much, albeit speaking decades before the rise of the surveillance state. In *United States v. Knotts*, which involved the use by police of tracking beepers, responding to defendant's argument that tracking beepers made the police too efficient, the Court rejoined, "Insofar as respondent's complaint appears to be simply that scientific devices such as the beeper enabled the police to be more effective in detecting crime, it simply has no constitutional foundation. We have never equated police efficiency with unconstitutionality, and we decline to do so now." 460 U.S. 276, 284 (1983).

Once we shift our view from privacy to power, we can better articulate the need for mandated police inefficiency. General warrants were powerful tools of efficiency, yet they went too far toward permitting arbitrary exercises of power on the colonies and tread too much on the liberties of the colonists. Today, with new technology, the police can often come close to exerting the power of the general warrant, as I have argued in a slightly different context.[141] A new Fourth Amendment attuned to problems of government power might need to resort to mandated police inefficiency in response.

D. Beyond Warrants and Probable Cause

Equilibrium adjustment can help judges determine whether to turn the Fourth Amendment's tuning knobs to restore the level playing field. But it will not do enough to safeguard liberty from undue governmental power unless we also add a few new tuning knobs.

A new Fourth Amendment designed to enforce the level playing field must address the misconception that the warrant and probable cause requirements represent the high water mark, the most onerous and liberty-protective things that may be imposed on the government. The very development that brought us to this point, the rise of the surveillance society, instead reveals that the warrant and probable cause requirements are often quite toothless requirements that the government will be able to meet with ease. It is a good thing that in their wisdom (or with luck), the Framers did not bind the Fourth Amendment solely to warrant and probable cause but instead required the much more flexible requirement of reasonableness.[142]

---

[140] Carroll v. United States, 267 U.S. 132, 151 (1925).

[141] Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1, 11 (2011), http://www.virginialawreview.org/inbrief/2011/03/20/ohm.pdf ("Computer search warrants are the closest things to general warrants we have confronted in the history of the Republic.").

In earlier work, I have argued that too much attention has been paid to the probable cause requirement.[143] Especially in debates over the proper Fourth Amendment requirements for access to electronically stored information like e-mail, the only requirement that gets serious attention is whether or not the police must show probable cause before access is allowed.

But I have argued that investigations that take place on networks differ from those in the physical world in five ways that all conspire to give the police probable cause in most circumstances:

> First, evidence online almost always comes surrounded by a rich context, providing a high level of built-in suspicion to a suspicious e-mail or IP address. Second, the path from victim back to suspect is fixed and often traceable. Third, the "eye witnesses" online tend to be sophisticated corporate intermediaries without relevant biases or agendas. Fourth, these intermediaries and the victims themselves deploy pervasive systems of surveillance. Fifth, these surveillance systems record precise, unambiguous evidence.[144]

All five of these features apply to the systems of private surveillance discussed in Part I. As the police shift from self-help to outsourced surveillance, and as they morph from producer to consumer of surveillance data, they will often find themselves awash in probable cause. Increasingly, it will seem odd to us that probable cause once seemed like an onerous burden. As the probable cause and warrant requirements cease playing a meaningfully disciplining role in many contexts, courts should find within the Fourth Amendment's requirement of "reasonableness" many additional requirements.

For ideas on what other types of restrictions on the police reasonableness might require, courts should look to Congress. One good source for such restrictions is the Electronic Communications

---

[142] Amar, *supra* note 74, at 762-85 (arguing against the pervasive idea that the Fourth Amendment requires warrants and probable cause).

[143] *See* Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514 (2010).

[144] *Id.* at 1529.

Privacy Act (ECPA).[145] In this law, Congress has found many other parameters to control aside from the mere suspicion standard. Some parts of this law require notice to the person whose records are being requested[146] and others do not.[147] Some require judicial review,[148] while others require only internal approval.[149] Among the parts of this law that require judicial review, some require searching review,[150] while others are much more minimalist.[151] Some surveillance can be conducted only in certain types of criminal investigations.[152]

In addition to all of these, the courts should consider availing themselves of a tuning knob that they have too rarely deployed, the necessity requirement, as I have argued elsewhere.[153] The necessity rule is a rule about timing. The rule provides that the court has deemed that a given police procedure is so invasive that the police must refrain from using it until late (or last) in their investigation.

Congress, again, has modeled the need for and efficiency of the necessity requirement in the federal wiretap act. Section 2518(c), Title 18 of the United States Code requires that the application for warrant include "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."[154]

If a particular type of private surveillance tilts the balance of power in favor of the police too far, the court can find within the Fourth Amendment's requirements a new necessity rule: when the police seek to monitor the records created by the third-party provider in the particular context (say location information), it should be required to first show that "other investigative procedures have been tried and failed . . . [or are] unlikely to succeed if tried or to be too dangerous."[155] Just because my smartphone tracks my location, this does not give the police the right to follow me around town when they could tail my car or install a tracking beeper instead.

---

[145] ECPA was first enacted in 1986 as the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), and has been amended many times since. *E.g.*, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. 107-56, §§ 209(2), 210, 212(b)(1), 220(a)(1), 220(b), 115 Stat. 283, 285, 291, 292 (2001). The Act amended and added scattered provisions throughout Title 18.

[146] 18 U.S.C. § 2703(b)(1)(A) (2006).

[147] *Id.* § 2703(b)(1)(B).

[148] *Id.* § 2518.

[149] *Id.* § 2703(b)(1)(B) (permitting access to certain records with a mere subpoena).

[150] *Id.* § 2518(3).

[151] *Id.* § 3123(a)(1).

[152] *Id.* § 2516.

[153] Ohm, *supra* note 143.

[154] 18 U.S.C. § 2518(c) (2006).

Until the courts get around to implementing this kind of rule, Congress should consider doing it. A good candidate is cell phone location tracking. At the time this Article was written, at least four bills had been introduced in the then-current Congress, which focused on the emerging problem of cell phone tracking.[156] At least two of these would have imposed a probable cause warrant requirement on the police before they could obtain prospective records of cell phone tracking.[157] In addition, Congress should consider requiring proof of necessity. Cell phone tracking, just like wiretapping, should not be allowed until "other investigative procedures have been tried and failed."[158]

The courts should learn an important lesson from the many tuning knobs of ECPA: there are many ways to rebalance the playing field of criminal investigation beyond the warrant and probable cause requirements, and the Fourth Amendment can incorporate them. The courts should feel free to superintend police procedures in new, creative ways, following Congress's lead. This is true no matter which way the playing field has tipped, either in favor of the police or the criminals. Let us consider each case in turn.

In situations when the metrics suggest that a new tool has tilted the playing field to criminals too much, making investigations much longer or increasing the number of unsolved crimes, rather than rolling back all Fourth Amendment protections, the Courts should consider stepping to a middle ground by requiring the kind of sub-warrant judicial approval embodied in ECPA's "d-order" standard.

---

[155] *Id.*

[156] Location Privacy Protection Act of 2011, S.1223, 112th Cong. (2011); Geolocation Privacy and Surveillance ("GPS") Act, S.1212, 112th Cong. (2011); Electronic Communications Privacy Act Amendments Act of 2011, S.1011, 112th Cong. (2011); Commercial Privacy Bill of Rights Act, S.799, 112th Cong. (2011).

[157] S.1212 § 2; S.1011 § 5.

[158] 18 U.S.C. § 2518(c) (2006).

According to 18 U.S.C. § 2703(d), some types of surveillance are permitted only when the government "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[159] Many have compared this to the standard of *Terry v. Ohio*, the stop-and-frisk standard that allows limited police inspection with less than probable cause.[160]

On the other hand, when a warrant requirement backed by the probable cause standard is found not to be enough, and a new technology made available by private providers shifts the playing field too far toward the government, making the police so hyper-efficient that it offends the balance of power promised by the Fourth Amendment, courts should feel free to require additional burdens on the police, such as new necessity requirements.

E. Putting the Pieces Together

1. The Default Rule

We are left with the problem of the default rule. When we are faced with very new technological advances, and before we know whether these advances have aided law enforcement or criminals more, should the rules impose significant burdens on the police, zero burdens on the police, or something in between? One way we can choose is to ask who should bear the cost of errors.

Today's default rule, in the form of the third-party doctrine, places the cost of errors on society not the police. In most emerging situations, the police can access the fruits of private surveillance without a warrant or probable cause.

The opposite result is the better one. The cost of errors should be borne first by the police. Whenever a private company enables a new form of surveillance, the police should be forced to assume that access to the fruits of the surveillance require a warrant and probable cause until we know (with the assistance of metrics) that the new service benefits criminals more than it helps the police.

---

[159] *Id.* § 2703(d).

[160] United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008); ORIN S. KERR, COMPUTER CRIME LAW 515-16 (2006); U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 131 (3d ed. 2009), *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf.

A textual analysis of the amendment supports this conclusion. The amendment prohibits unreasonable searches and seizures. It does not guarantee for police the minimal burdens possible. The right is for the investigated not the investigator.[161] If Congress passes a law permitting the search of a home without a warrant, the law is unconstitutional and void. On the other hand, if Congress passes a law forcing the use of a warrant in situations where the amendment would require none, this is fine, because it is well within the prerogative of legislatures to require more protection than the Constitution provides.

There is one last reason to favor this default rule. The metrics at issue will largely be controlled by the police. Creating a default rule of no process needed gives the police the incentive to drag their feet or obfuscate statistics. On the other hand, placing the benefit of delay against the party likeliest to delay will help improve the overall legitimacy and efficiency of the process.

2. Breaking the Link Between the Surveillance Society and State

Putting the pieces together, when a court must resolve a Fourth Amendment challenge to police access to information stored by a third party, particularly in cases involving new technologies like networked communications, the police must present statistics quantifying the effect the technology in question has had on criminal investigations. Having thus introduced the basic idea, this Article will not also proceed to try to identify the very best set of statistics to measure, which it expects to be the subject of much debate and litigation, should this approach ever be embraced.

If statistics are unavailable or hard to interpret because the technology is new, then the police may access the information only with a warrant and probable cause, because of the default rule. If the statistics indicate that the technology has greatly hampered law enforcement, by letting criminals evade detection by hiding once-visible activity online, then the court will decrease the requirements of the Fourth Amendment for access to the data, perhaps to a mere subpoena or by relaxing the requirement of notice to the user. Finally, if statistics indicate that even with a warrant and a probable cause, the technology has shifted the playing field too far to the benefit of the police, the court can impose new burdens on the police such as a requirement of necessity.

---

[161] Similarly, Morgan Cloud, considering the "two conflicting value-based assumptions" of the Fourth Amendment, one which "favors efficient law enforcement, the other favors individual liberty," chose liberty "as the *grundnorm* of the amendment" based on the "history and text of the amendment." Cloud, *supra* note 93, at 296.

CONCLUSION

For nearly fifty years, privacy has served as a useful proxy for deciding what the Fourth Amendment protects. As we witness the rapid decline of privacy, we should be prepared to rebuild the Fourth Amendment on a new foundation focused on the balance of power between the state and its citizens.

The shift from privacy will be a disruptive one, and we will be forced to abandon long-held intuitions and maxims. One especially important one that deserves some attention before we let it go is the centuries-old maxim that police on the street need not "avert their eyes" from crime in public.

The maxim is ancient and was already established by the time Lord Chief Justice Camden wrote in *Entick v. Carrington* that "the eye cannot by the laws of England be guilty of trespass."[162] It is hard to argue with the logic behind it. There is a deeply intuitive appeal to the idea that we cannot ask police officers, sworn to protect and thrust in harm's way, to ignore what is right in front of them. It is hard to believe that the Framers would have intended such a result. Forcing the police to shift their eyes in physical, public places seems an unwise shift in the constitutional balance between privacy and security.

---

[162] 19 How. St. Tr. 1029 (1765), 95 Eng. Rep. 807 (K.B. 1765). The full quote lends support for the argument that the police need limits with respect to private papers:

> Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect. Where is the written law that gives any magistrate such a power? I can safely answer, there is none; and therefore it is too much for us without such authority to pronounce a practice legal, which would be subversive of all the comforts of society.

19 How. St. Tr. 1029 (1765).

But once you move from a Fourth Amendment built on privacy to one built on power, the unassailable logic breaks down. We certainly have never presupposed that the police are entitled to every fact about behavior on earth. The list of the things the police officer on the sidewalk is prevented from learning about the activity in the immediate vicinity is much, much longer than the list of facts he can observe, because he is subject to two types of constraints, one set by the laws of physics, the other by the laws of man. On the sidewalk, the laws of physics predominate. Things happening behind walls and closed doors are unseen; conversations whispered a block away or coursing through the wires overhead are unheard; and heat patterns emanating through walls are undetected. The world—the physical world—is rich with natural, physical constraints like these.

Technology can war with physics, giving the police the ability to enhance their senses, making natural constraints irrelevant. With a wiretap, the police can listen to the conversations on the wires, and with a thermal imager, the police can detect invisible heat patterns. But in both of these cases, the Supreme Court has decided that these tools upset the constitutional balance toward security and away from privacy too much, and it has replaced the vanished physical constraint with a legal constraint.[163]

Consistent with these cases, we should view the police officer on the sidewalk as a complicated story of constraints, some imposed by physics and some by law. I am arguing that today, many structural constraints are falling away.[164] Until the recent past, business practices (and the laws of physics) provided many well-tailored "structural rights in privacy."[165] Private companies, by convincing us all to carry tracking beepers and to post status updates, have knocked down these structural rights in privacy.

---

[163] Kyllo v. United States, 533 U.S. 27, 40 (2001); Katz v. United States, 389 U.S. 347, 358-59 (1967).

[164] *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009); Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605 (2007).

[165] Surden, *supra* note 164, at 1617-18.

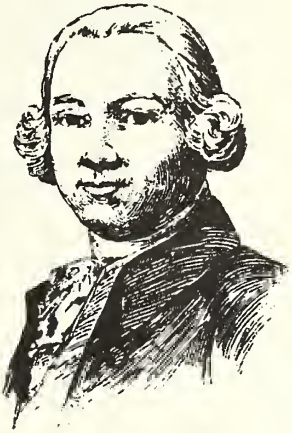
Now that we are losing structural constraints of privacy, sometimes the Fourth Amendment might force the police to avert their eyes to easily and readily obtainable facts, just as it has done in other contexts.[166] But where wiretapping and thermal imaging used to seem the exception not the rule, soon, our default stance should be to deny the police easy access to newly revealed facts out in the world. This is not unnatural, nor embarrassing, nor regrettable. It is the direct consequence of the new Fourth Amendment, which polices power not privacy, and one which serves as an important bulwark of liberty in these changing times.

---

[166] *Cf.* David A. Sklansky, *Back to the Future:* Kyllo, Katz, *and Common Law*, 72 MISS. L.J. 143, 210 (2002) ("In the long term, sensible interpretation of the Fourth Amendment will require the Court to acknowledge the differences between government surveillance and private snooping, and to abandon the assumption that anything knowingly exposed 'to the public' is therefore fair game for the police.").

The James Otis Lectures

ANNUAL LECTURE SERIES



This lecture series is fittingly named after the man who not only ignited the American Revolution, but whose very words in opposition to the writs of assistance inspired much of the language of the Fourth Amendment, James Otis.

Born in Great Marshes (now West Barnstable), Massachusetts, Otis would devote his life to the law, as his father and grandfather had done before, becoming a revered trial advocate and legal orator in colonial Massachusetts. He was appointed to the coveted position of Advocate General of the Vice-Admiralty Court at just thirty-one years of age, a position he would later resign to champion the cause against the Crown's arbitrary issuance of writs of assistance. The writs were general search warrants that permitted the authorities to search anywhere they pleased for any reason—or for no reason. In one of the first defiant stands against British authority in the Colonies, Otis attacked the writs as "'against the fundamental principles of law.'"[1] He asserted, among other things: "A man's house is his castle; and while he is quiet, he is as well guarded as a prince in his castle. This writ, if it should be declared legal, would totally annihilate this privilege."[2] Importantly, Otis articulated for the first time in history a comprehensive view of what search warrants should require: an oath; a particular description of the place to be searched and things to be seized; and probable cause to justify the intrusion.

---

[1] TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 36-37 (1969) (quoting John Adams, Petition of Lechmere, *in* 2 LEGAL PAPERS OF JOHN ADAMS 125 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965)).

John Adams, who witnessed Otis's impassioned oration, afterward declared: "Every man of an [immense] crowded [a]udience appeared to me to go away, as I did, ready to take [a]rms against [Writs] of Assistance. Then and there was the first scene of the first [a]ct of [o]pposition to the arbitrary [c]laims of Great Britain. Then and there the child Independence was born."[3]

Although Otis may have lost his case before the Massachusetts Superior Court in Boston's Old Town Hall that day, he gained a place in history. In that case, "the American tradition of constitutional hostility to general powers of search first found articulate expression."[4] It was Adams, so inspired by Otis's words, who later drafted Article Fourteen of the Massachusetts Declaration of Rights of 1780, which served as the model for the Fourth Amendment.[5]

Although eventually reduced to insanity and ultimately silenced by a bolt of lightning, James Otis will forever remain first among America's Fourth Amendment advocates.

*Thomas K. Clancy**

---

[2] *Id.* at 37 (quoting John Adams, Petition of Lechmere, *supra* note 1, at 142).

[3] John Adams, Petition of Lechmere, *supra* note 1, at 107.

[4] M.H. Smith, THE WRITS OF ASSISTANCE CASE 7 (1978).

[5] *See generally* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979 (2011).

* Director, National Center for Justice and the Rule of Law. The Center, and consequently this lecture series and articles stemming from it, is supported by grants awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in the articles are those of the author and do not represent the official position of the United States Department of Justice.

ELECTRONIC PRIVACY IN THE GOVERNMENT WORKPLACE AND *CITY OF ONTARIO, CALIFORNIA V. QUON*: THE SUPREME COURT BROUGHT FORTH A MOUSE

Clifford S. Fishman[*]

INTRODUCTION 1361
I. THE FOURTH AMENDMENT AND RELEVANT FEDERAL STATUTES 1363
  A. Fourth Amendment 1363
    1. Reasonable Expectation of Privacy....................... 1363
    2. Situations in which a Person Surrenders his Reasonable Expectation of Privacy 1366
  B. Statutory Regulation of Surveillance of

---

[*] Professor of Law, The Columbus School of Law, The Catholic University of America. B.A., University of Rochester, 1966; J.D., Columbia Law School, 1969. From 1969 to 1977, Professor Fishman served as an Assistant District Attorney in the New York County District Attorney's Office and as Chief Investigating Assistant District Attorney in New York City's Special Narcotics Prosecutor's Office, where he tried dozens of cases, drafted and supervised the execution of more than forty wiretaps and eavesdrops and, among other triumphs, oversaw the purchase of the most expensive pound of pancake batter in the history of American law enforcement. Having cleaned up New York City's drug problem, he joined the faculty at Catholic University in 1977. He is the co-author of two multi-volume legal treatises which, together with his eighteen prior law review articles, contain more footnotes than any rational human being would ever read in one lifetime, let alone write. Professor Fishman expresses his gratitude to the National Center for Justice and the Rule of Law at the University of Mississippi School of Law, and to Tom Clancy, its director, for the honor of being chosen to give the James Otis Lecture in October, 2010. This Article is an outgrowth of that lecture. Prof. Fishman also wants to thank his treatise co-author, Anne T. McKenna; his research assistant, Eduardo Bertran, J.D., C.U.A. Law School, 2011; C.U.A. Law librarian Steve Young; and his C.U.A. faculty colleagues, Professors Cara Drinan and Mary Leary, for their assistance in researching and drafting this Article. Thanks, too, go to his administrative assistant, Julie Kendrick, for her help in this and in every other professional project he undertakes. Finally, Professor Fishman also wishes to acknowledge Washington, D.C.'s NFL, NBA, and MLB franchises, whose persistent mediocrity over the past few decades eliminated many distractions that might have interfered with his footnote production.

Communications 1368
    1. Title III 1368
    2. The ECPA and SCA 1369
    3. Other Legislation 1370
C. Measuring the Validity of a Search 1371
    1. The Warrant Requirement and Probable Cause 1371
    2. Administrative, Regulatory, and Other "Special Needs" Searches 1373
II. *O'CONNOR V. ORTEGA* 1376
A. Facts and Issues 1376
B. Reasonable Expectation of Privacy 1379
C. Appropriate Standard to Determine "Reasonableness" 1380
    1. Justice O'Connor's Plurality Opinion 1380
    2. Justice Scalia's Concurrence 1382
    3. Dissent 1383
III. *CITY OF ONTARIO V. QUON* 1384
A. Facts 1384
B. The Technology 1388
C. The Ninth Circuit Decision 1388
D. The Supreme Court Decision: Overview 1389
E. The Majority Opinion 1391
    1. Three Assumptions 1391
    2. The OPD Review of the Transcripts was Reasonable; Applying the *O'Connor* Plurality Approach 1392
    3. Availability of "Less Intrusive Means" 1394
    4. The Stored Communications Act (SCA) and the Fourth Amendment 1399
    5. Conclusion; Lip Service Deference to Justice Scalia's *O'Connor* Concurrence 1403
F. Justice Scalia's Quon *Concurrence* 1404
IV. WHAT THE COURT DID NOT DECIDE, AND WHY: EXPECTATIONS AND STANDARDS 1405
A. Measuring Expectations of Electronic Privacy 1406
    1. The Majority's Waffle: Part III.A of the Court's Opinion 1406
    2. Justice Scalia's "I Told You So" 1408

3. Evaluation; Comparing the Two Approaches........1409
4. The Need for Legislation..1415
B. Suppose the Jury Had Found That the Review Was to Investigate Suspicions of Quon's Wrongdoing.....1418
C. Privacy Expectations of Those With Whom Quon Texted..1419
CONCLUSION 1424
APPENDIX. *QUON*: A USER'S MANUAL 1427

> Many years ago a mighty rumbling was heard from a mountain, which was said to be in labour. Thousands of people flocked from far and near to see what it would produce. After a long time of waiting in anxious expectation—out popped a mouse![1]

INTRODUCTION

A company gives an employee (E) a cellular phone to use on company matters. The phone is programmed to send and receive text messages. E is told that he may send and receive up to a certain number of alphanumeric characters per month, with no cost to E. The company makes a point of informing E that it reserves the right to review his use of the phone, including the text messages he sends and receives. Informally, however, his supervisor tells him that the company will not enforce this policy; instead, personal use of the phone and text messaging will be permitted, so long as E pays for any text message use that exceeds the contractual character limit per month. Does this informal understanding give E a right to privacy in the personal text messages he sends and receives? If so, and the company decides to review E's text messages, does it matter why the company did so? And what about the people who send text messages to E, and receive messages from him—do they have any right to privacy against the company's review of the messages? Does it matter whether those with whom E texts are aware that E is using a company phone, rather than his personal phone?

Suppose instead E works for a government agency—local, city, state, or federal. Would the privacy issues raised in the previous paragraph be resolved any differently? If so, how and why?

---

[1] *The Mountain in Labour*, *in* AESOP'S FABLES 31 (Jack Zipes ed., 1992).

The Supreme Court confronted these issues in 2010 in *City of Ontario v. Quon.*[2] Sergeant Jeff Quon sued his employer, the Ontario Police Department, when he learned that the OPD reviewed the text messages he had sent and received on a department-issued pager.[3] The Ninth Circuit entered judgment for Quon;[4] the city appealed to the Supreme Court. The Court's decision in that case touches on a wide range of social, technological, and legal issues, including: (1) the role various electronic communications media play in our lives; (2) whether a government employee has a reasonable expectation of privacy when he uses equipment or systems provided by the government agency for which he or she works; (3) when, assuming such an expectation exists, the government employer is nevertheless justified in intruding upon that privacy; and (4) the legal standard against which those expectations and justifications are to be measured.

Quon is the third time the Supreme Court has addressed the issue of a government employee's right to workplace privacy from the agency that employs him or her. The first was *O'Connor v. Ortega*,[5] decided in 1987. That decision recognized an employee's rights to privacy, but provided no clear guidance as to how those rights are to be measured;[6] nor did the second decision, *National Treasury Employees Union v. Von Raab*,[7] decided in 1989, because although *Van Raab* did involve the employer-employee relationship, it is better understood when viewed from a different legal perspective.[8] When the Court granted cert in *Quon*, therefore, many scholars, judges, and practitioners hoped that the *Quon* decision would clarify the uncertainties left over from *O'Connor* and resolve new issues created by electronic communications technology. On the other hand, some observers feared that the Court in *Quon* might issue a broad, sweeping decision that could have a substantial, unforeseeable, and perhaps unfortunate impact on emerging communications technologies. As it turned out, *Quon* decided very little, and leaves the law more unsettled than it previously was.

---

[2] City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010). *Quon* involved an alphanumeric pager, rather than a cell phone with texting capability. Cell phones with text-message capacity are probably now far more widely owned and used than pagers, and the issues presented by the text messages in *Quon* would apply equally to text messages sent by phone.

[3] *Id.* at 2621-22.

[4] Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008). See *infra* Part III.A and Part III.C for a more detailed discussion of the district court and circuit court decisions.

[5] O'Connor v. Ortega, 480 U.S. 709 (1987).

[6] See *infra* Part II for an extensive discussion of *O'Connor*.

[7] Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656 (1989).

[8] See *infra* notes 121-22 and accompanying text for discussion of *Von Raab*.

This Article will begin with a very brief overview of fundamental Fourth Amendment principles and federal statutory regulation of electronic surveillance of communications. Part II consists of a detailed look at *O'Connor v. Ortega*, and the uncertainties the decision created in the law. Part III will examine the *Quon* case, and analyze what the Court did decide. Part IV examines the issues in *Quon* that the Court did *not* decide. Part V states my conclusions as to where the decision leaves the law. The Article ends with an "user's guide" to *Quon*, which outlines how litigants and judges should attempt to apply *Quon* if presented with a case involving privacy in the government or private sector workplace.

I. THE FOURTH AMENDMENT AND RELEVANT FEDERAL STATUTES

A. Fourth Amendment

1. Reasonable Expectation of Privacy

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[9]

---

[9] U.S. CONST. amend. IV.

It is clear from the language of the amendment that, to determine the scope of Fourth Amendment protection, it is necessary to define its key terms: "search" and "seizure." Application of the term "seizure" to some forms of electronic surveillance raises difficult questions,[10] but for purposes of this Article, its application is fairly straight-forward: a seizure occurs when someone acquires physical possession of either a printed or an electronic copy of a communication such as an e-mail, text message, etc.

One major focus of this Article is what constitutes a "search" in the workplace. Until the mid-1960s, legal definitions of "search," for Fourth Amendment purposes, focused upon whether a government investigator had intruded or trespassed upon a "constitutionally protected area."[11] The prevailing doctrine was that a Fourth Amendment "search" occurred only if the government physically intruded into such an area and thereby breached the defendant's "right to privacy."[12]

---

[10] For example, is a phone call "seized" if it is overheard by someone listening in on an extension phone or wiretap, or only when it is recorded? For a discussion of this issue, see CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE § 1:5 (3d. ed. 2007). Federal and state statutes regulating electronic surveillance finesse the issue by regulating, not the "seizure" of communications, but their "interception," which is defined broadly to include any "real time" acquisition of the contents of wire communications (i.e., telephone conversations), oral communications (i.e., face-to-face conversations), and electronic communications (i.e., e-mails, tweets, etc.), by means of any electronic, mechanical, or other device. *See* 18 U.S.C. § 2510(4) (2006) (definition of "intercept"). For a detailed analysis of this definition and related terms, see *id.* at §§ 2:61-2:110.

[11] *See* Hoffa v. United States, 385 U.S. 293, 301 ("What the Fourth Amendment protects is the security a man relies upon when he places himself or his property within a constitutionally protected area, be it his home or his office, his hotel room or his automobile."). The Court considered whether the government violated defendant Hoffa's Fourth Amendment rights when Edwin Partin, an acquaintance of Hoffa's, gained entrance to Hoffa's hotel room by concealing the fact that he was acting as a government informant. The Court held that no violation occurred because when Hoffa admitted Partin he assumed the risk that Partin might be an informant (Partin's testimony played a central role in convicting Hoffa of tampering with the jury in the case for which he had been on trial.). For a detailed discussion of the *Hoffa* case, see VICTOR S. NAVASKY, KENNEDY JUSTICE 418-24 (1971); *see also* Lopez v. United States, 373 U.S. 427 (1963). Lopez offered a bribe to IRS agent Davis to help resolve a tax matter; thereafter Davis went to Lopez's office, ostensibly to seal the deal, carrying a wire recorder which recorded the conversation. In upholding the admissibility of the recording, the Court commented that the Fourth Amendment protected against surreptitious electronic overhearing "only [if] the electronic device [is] planted by an unlawful physical invasion of a constitutionally protected area," *Lopez*, 373 U.S. at 348-439, and held that because Lopez had invited Davis into his office, there had been no unlawful "invasion" of the office. *Id.*; *see also* Lanza v. New York, 370 U.S. 139, 142 (1962) (holding that it did not violate the Fourth Amendment to surreptitiously record

In 1967, in *Katz v. United States*, the Court rejected this "formulation" of what the Fourth Amendment protected.[13] Rather, Justice Stewart stated in his majority opinion:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . [b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[14]

Thus, the Court held that when Katz closed the glass door to a public phone booth, although he was *visible* to the public, the Fourth Amendment protected what he said from the uninvited listener.[15]

---

defendant's conversation with his brother in the visitors' room of a public jail, because that location was not a "constitutionally protected area.").

[12] The phrase "right to privacy" has a long and storied history. The phrase became common in American legal jurisprudence as a result of Samuel D. Warren and Louis D. Brandeis's famous article, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). That article is considered by many legal scholars to be the seminal work in the area of privacy rights and is still cited over a hundred years later. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 534 (2000); Toffoloni v. LFP Publ'g Grp., LLC, 572 F.3d 1201, 1206 (11th Cir. 2009); Brown v. Mortensen, 253 P.3d 522, 526 (Cal. 2011); Tarlton v. Kaufman, 199 P.3d 263, 273 (Mont. 2008) (Morris, J., dissenting). Interestingly enough, the phrase, "right to privacy," has also had its detractors. *See* Erin Miller, *Justice Stevens and the So-called Right to Privacy*, SUPREME COURT OF THE UNITED STATES BLOG (May 21, 2010, 3:07 PM), http://www.scotusblog.com/2010/05/justice-stevens-and-the-so-called-right-to-privacy/ (noting that the phrase "so called 'right to privacy'" first appeared in a 1902 decision by New York's highest court).

[13] Justice Stewart wrote:

> We decline to adopt this formulation of the issues. In the first place the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase "constitutionally protected area." Secondly, the Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion.

Katz v. United States, 389 U.S. 347, 350 (1967) (footnotes omitted).

[14] *Id.* at 351.

[15] *Id.* at 358-59.

Justice Harlan, concurring, pointed out that it is usually difficult to apply the Fourth Amendment without reference to the place in which the government surveillance occurred.[16] He read the Court's prior decisions as creating the rule that to enjoy Fourth Amendment intrusion from government surveillance, "there is a twofold requirement, first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[17] Although the *Katz* majority rejected the concept that Fourth Amendment protection and "privacy" were equivalent concepts,[18] the Supreme Court has since adopted the second part of Justice Harlan's formulation, and has held on several occasions that the Fourth Amendment protects only reasonable (or legitimate) expectations of privacy,[19] although in 2001, the Court acknowledged that the reasonable expectation of privacy test "has been criticized as circular, and hence subjective and unpredictable."[20]

2. Situations in which a Person Surrenders his Reasonable Expectation of Privacy

Over the years, the Supreme Court has recognized a variety of situations in which a person loses what otherwise would be a reasonable expectation of privacy. The Court articulated one such situation in *Katz*: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[21]

---

[16] *Id.* at 361 (Harlan, J., concurring).

[17] *Id.* (Harlan, J., concurring) (internal quotation marks omitted).

[18] *Id.* at 350; *see supra* text accompanying note 13.

[19] *See, e.g.*, California v. Greenwood, 486 U.S. 35, 41 (1988) (holding defendant had no reasonable expectation of privacy in garbage set out on the curb for collection); Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that it did not intrude into Smith's reasonable expectation of privacy when the phone company made a record of the numbers he dialed from his home phone and turned the information over to the police).

[20] Kyllo v. United States, 533 U.S. 27, 34 (2001). The Court, per Justice Scalia, held that a person has a reasonable expectation of privacy against government use of surveillance equipment to learn any information about the inside of his home, at least if the equipment was not readily available to the general public, and therefore the use of a thermal imaging device to measure the amount of heat emanating from Kyllo's home was a search which, in the absence of a search warrant, violated that expectation. *Id.*

Second, if a person consents to a search, the search is lawful.[22] The validity of consent is based on an assessment of all of the relevant circumstances.[23] In reality the term "consent" is a misnomer. The Supreme Court has held that a person's "consent" to a search is valid even though the officer did not inform the person of his right to refuse.[24] In essence, the officer may exploit the suspect's ignorance and the inherently coercive nature of the police-civilian encounter.[25] It suffices that—considering a totality of the circumstances[26]—the officer obtained the person's acquiescence to the search without engaging in overtly coercive conduct.[27] The consent-to-search concept also applies in the sometimes coercive employer-employee context as well.[28]

Third, whenever a person confides in someone else, he assumes the risk that individual is now working with or may later disclose the confidence to the authorities.[29]

---

[21] Katz v. United States, 389 U.S. 347, 351 (1967).

[22] Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973); *see also* United States v. Drayton, 536 U.S. 194, 207 (2002) ("In a society based on law, the concept of agreement and consent should be given a weight and dignity of its own. Police officers act in full accord with the law when they ask citizens for consent. It reinforces the rule of law for the citizen to advise the police of his or her wishes and for the police to act in reliance on that understanding. When this exchange takes place, it dispels inferences of coercion.").

[23] *Schneckloth*, 412 U.S. at 227.

[24] *Id.*; *Drayton*, 536 U.S. at 203.

[25] The Court has never explicitly stated, but this is the clear implication of cases such as *Florida v. Bostic*, 501 U.S. 429, 438 (1991). In *Bostic*, the defendant quite plausibly argued that no one in his right mind would consent to a search, knowing the police would find contraband, and the defendant's acquiescence to the search therefore must have been coerced. *Id.* at 435. The Court rejected this argument, holding that whether the police acted coercively was to be viewed from the perspective of a reasonable, innocent person in the defendant's situation. *Id.* at 437-38.

[26] *Drayton*, 536 U.S. at 207.

[27] *See Drayton*, 536 U.S. at 207; *Schneckloth*, 412 U.S. at 219.

[28] *See infra* Part III.A.

[29] *See* Hoffa v. United States, 385 U.S. 293 (1966); Lopez v. United States, 373 U.S. 427 (1963). In *United States v. White*, 401 U.S. 745 (1971), the Court held that an undercover agent did not violate White's Fourth Amendment rights when he surreptitiously transmitted to other agents his conversations with White in a variety of locations, including White's home.

B. Statutory Regulation of Surveillance of Communications

1. Title III

Congress responded to *Katz* and another Supreme Court decision, *Berger v. New York*,[30] by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[31] Designed to protect the privacy of wire and oral communications,[32] Title III made it a crime for private persons to intercept such communications, and forbade law enforcement officials to do so without a court order,[33] usually referred to as an "interception order." The legislation mandates that to obtain such an order, the prosecutor must submit an application to a judge that satisfies not only the Fourth Amendment requirements for a search warrant, but several additional conditions as well.[34] For example, an interception order may not be submitted to a federal judge unless it is first approved by a high-level official of the U.S. Department of Justice;[35] applications by state officials to a state judge must first be approved by the state attorney general, the county's chief prosecutor, or specific assistants designated by them.[36] An interception order may be sought and issued only where probable cause exists[37] for particularly serious, statutorily designated crimes.[38] The application must establish that other investigative procedures have been tried and failed, would be unlikely to succeed, or would be too dangerous.[39] The orders must be executed to "minimize the interception" of communications unrelated to the crimes being investigated.[40]

---

[30] 388 U.S. 41 (1967). The Court held New York's wiretapping statute unconstitutional because it was overly broad, lacked particularization with regard to what conversations could be listened to, authorized the indiscriminate use of electronic devices, and allowed for extension of the eavesdropping based solely on a showing that an extension was in the public interest. *Id.*

[31] 82 Stat. 197 (1968) (codified at 18 U.S.C. §§ 2510-2522 (2006)).

[32] Electronic communications were added to the statute as part of the Electronic Communications Privacy Act of 1986.

[33] 18 U.S.C. § 2511(1) (2006).

[34] *See generally* 18 U.S.C. § 2518 (2006). For an exhaustive discussion of this provision, see FISHMAN & MCKENNA, *supra* note 10, chs. 8-11.

[35] 18 U.S.C. § 2516(1) (2006) (wire and oral communications); *see* FISHMAN & MCKENNA, *supra* note 10, § 8:5. 18 U.S.C. § 2516(3) (2006) (electronic communications); *see* FISHMAN & MCKENNA, *supra* note 10, § 8:6.

[36] 18 U.S.C. § 2516(2) (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 8:7-8:11.

[37] 18 U.S.C. §§ 2518(1)(b), 2518(3)(a), (b), (d) (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 8:53-8:70.

[38] 18 U.S.C. § 2516(1) (2006) (federal orders); 18 U.S.C. § 2516(2) (state orders); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 8:35-8:40.

Where a participant to the communication consents to its interception, however, the interception is lawful and no court order is needed.[41]

2. The ECPA and SCA

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA).[42] As its title implies, a primary purpose of ECPA was to protect the privacy of electronic communications from unauthorized acquisition by either private individuals or government agents.[43]

A major component of ECPA are provisions, codified at 18 U.S.C. §§ 2701-11, which regulate the disclosure of stored electronic communications such as e-mails and text messages. These provisions are often referred to as the "Stored Communications Act" (SCA).[44] The SCA makes it a crime to access stored wire or electronic communications without legal authorization.[45] Penalties for violating the statute range from six months' to two years' imprisonment and fines ranging from $5000 to $250,000.[46] It is also unlawful for an individual or entity involved in the transmission or storage of the communication to improperly divulge the contents of such a communication.[47] Unauthorized access to or divulgence of stored communications is also civilly actionable.[48]

---

[39] 18 U.S.C. § 2518(1)(c) (2006) (application); 18 U.S.C. § 2518(3)(c) (order); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 8:71-8:92.

[40] 18 U.S.C. § 2518(5) (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 8:101-8:107.

[41] 18 U.S.C. § 2511(2)(c) (2006) (interceptions with the consent of a participant are lawful if made "under color of law"); 18 U.S.C. § 2511(2)(d) (interceptions by private individuals with the consent of a participant are lawful so long as the interception was not done for the purpose of committing a crime or a tort); *see* FISHMAN & MCKENNA, *supra* note 10, ch. 5.

[42] 18 U.S.C. §§ 1367, 2521, 2701-11, 3117, 3121-37 (2006).

[43] Among other things, ECPA amended Title III, *see supra* Part I.B, to make it a crime, and civilly actionable, for a private person or entity to intercept electronic communications as they are being transmitted. 18 U.S.C. § 2511(1) (2006).

[44] An astute reader (or one with nothing better to do) may have noticed that although the SCA and ECPA are both statutes, I refer to them as "the SCA" (with a "the") and "ECPA" (without a "the"). I do so because when "ECPA" is referred to aloud, it is usually pronounced as if it was a word—"Eck-pa"—without the "the," while the SCA is pronounced "the S-C-A."

[45] 18 U.S.C. § 2701(a) (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 7:10-7:12. Where an employer is the service provider of an e-mail system for its employees, however, the employer may access stored or archived e-mail messages without the knowledge or permission of employees. This is so because 18 U.S.C. § 2701(1)(c) permits the service provider to do pretty much what it wants with regard to stored

The scope of the SCA was an important issue at the *Quon* trial and on appeal to the Ninth Circuit.[49] Although the Supreme Court declined to grant certiorari on the statutory issues,[50] the Court did discuss the relevance of the statute to the issues on which it did grant cert.[51]

3. Other Legislation

Congress has enacted other statutes protecting communicational privacy and regulating government access to private communications,[52] but these statutes do not play a role in the *Quon* case, and this Article will offer no discussion of them.[53]

---

communications. *See* FISHMAN & MCKENNA, *supra* note 10, § 7:21. However, this situation did not apply in *Quon*, because the communications service was provided by a corporate ISP, Arch Wireless Operating Company.

[46] 18 U.S.C. § 2701(b) (2006); *see* FISHMAN & MCKENNA, *supra* note 10, § 7:13.

[47] 18 U.S.C. § 2702 (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 7:33-7:34.

[48] 18 U.S.C. § 2707 (2006); *see* FISHMAN & MCKENNA, *supra* note 10, § 7:30. The statute likewise spells out the circumstances in which the government may obtain access to such communications as part of a criminal investigation. 18 U.S.C. § 2703 (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 7:45-7:55. Depending on the circumstances, the government may proceed either by search warrant, by subpoena, or by court order; the customer whose electronic "storage bin" is being pierced may receive prior notice that the government seeks access to stored records, thereby enabling the customer to move to quash the action; or he may receive notice only after the government has already obtained the records; or he may not receive notice at all. 18 U.S.C. § 2705 (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 7:57-7:58. These latter portions of the statute are not relevant to the *Quon* case, because the Ontario Police Department, Quon's employer, was not conducting a criminal investigation against Quon.

[49] *See infra* note 158.

[50] *See infra* Part III.D.

[51] *See infra* Part III.E.4.

[52] Government use of pen registers and trap-and-trace devices to record the numbers dialed by a particular phone, and the source of calls to that phone, is regulated by 18 U.S.C. § 2703(c), (d) and (e) and 18 U.S.C. § 3121-27; *see generally* FISHMAN & MCKENNA, *supra* note 10, ch. 4. Federal statutes protecting computer privacy include the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006). For detailed coverage of that and other computer-related legislation, see generally

C. Measuring the Validity of a Search

If a court concludes that government agents have conducted a Fourth Amendment search, the question then becomes whether the search was lawful. The Fourth Amendment does not prohibit all searches and seizures, it protects against only those which are unreasonable.[54] Other than the general requirement that to be lawful a search must not be "unreasonable," the only explicit guidance the amendment provides is that "no Warrants shall issue, but upon probable cause, particularly describing the place to be searched, and the persons or things to be seized."[55] The amendment does not define probable cause; nor does it explicitly state whether a search may be reasonable in the absence of probable cause; nor does it specify when a warrant is required.

1. The Warrant Requirement and Probable Cause

As to the latter issue, the operative cliché is that "as a general matter, warrantless searches are *per se* unreasonable under the Fourth Amendment," subject to "a few specifically established and well-delineated exceptions" to that general rule.[56] The Court has said so in almost exactly the same words twenty-four times[57]—once for each blackbird baked in the nursery rhyme pie.[58] But "saying it's so doesn't make it so."[59] In fact, the

---

FISHMAN & MCKENNA, *supra* note 10, ch. 25. The Foreign Intelligence Surveillance Act (FISA), codified at 50 U.S.C. §§ 1801-12, regulates (among other things) the use of electronic surveillance of communications for national security purposes. *See generally* FISHMAN & MCKENNA, *supra* note 10, ch. 12 (Incidentally, this statute is generally pronounced "FIE-SUH" and is not preceded by a "the."). States have also passed legislation regulating the interception of communications and related subjects. For extensive coverage of these statutes, see generally *id.* §§ 1-11, 13-41.

[53] The footnotes in Parts I.B and I.C may set a new world's record for frequency of professorial self-citation per word of text; if not, I'll bet they come close.

[54] U.S. CONST. amend. IV.

[55] *Id.*

[56] City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) (citations omitted) (internal quotation marks omitted).

[57] Anyone interested in the complete list need only do a Westlaw search, data base U.S. Supreme Court, for the phrase "per se unreasonable under the Fourth Amendment." A search including minor variations on this phrase would no doubt produce additional cases.

[58] The first two lines of the rhyme read, "Sing a song of six pence, a pocket full of rye. Four-and-twenty blackbirds baked in a pie." For the full text of the rhyme, its history (apparently at one time, enclosing live birds inside a pie was a popular custom),

exceptions to the warrant requirement are many rather than few,[60] and some are not at all well-delineated,[61] as even a superficial perusal of the leading treatises on the Fourth Amendment will quickly reveal.[62] The vast majority of searches conducted by government agents are lawful despite the absence of a warrant;[63] a substantial number of these are lawful despite the

---

theories concerning its deeper meaning, and cultural references to it in literature and popular culture (my reference to it in this Article enrolls me in a roster of luminaries including, among others, William Shakespeare and Paul McCartney), see *Sing a Song of Sixpence*, *in* THE OXFORD DICTIONARY OF NURSERY RHYMES 394-95 (Iona Opie & Peter Opie eds., Oxford Univ. Press 2d. ed. 1997) (1951); WILLIAM SHAKESPEARE, TWELFTH NIGHT act 2, sc. 3; THE BEATLES, *Blackbird*, *on* THE BEATLES (Apple Records 1968).

[59] I tried to find the original source for this phrase. My edition of BARTLETT'S FAMILIAR QUOTATIONS did not list it in the index. A Google search produced 14,600 hits. I examined the first several; none cited the original source. I would have dutifully continued down the list, but my wife insisted that I help put away the Passover dishes.

[60] Examples: search of the person incident to arrest; search of the area incident to arrest; stop-and-frisks; searches conducted during hot pursuit of a fleeing suspect; searches conducted to prevent the impending destruction of evidence; searches of vehicles; searches of containers in vehicles; consent searches; and an impressive variety of inspection, regulatory, and other "special needs" searches. *See* discussion *infra* Part I.C.2.

[61] Consider, for example, the search-of-the-area incident to arrest doctrine first announced in *Chimel v. California*, 395 U.S. 752 (1969), in which the Court held that at least in some circumstances, after the police have arrested someone within a premises, they may search the immediate area for weapons or destructible evidence. Lower courts have debated ever since whether the right to conduct such a search continues after the arrestee has been secured and moved to a different location. The Supreme Court returned to that issue in *Arizona v. Gant*, 129 S. Ct. 1710 (2009), a case involving the search of an automobile, in which the plurality and dissenting opinions each cited *Chimel* more than twenty times, without clarifying the issue much, if at all.

[62] *See, e.g.*, THOMAS CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION ch. 6 (2008) (discussing arrests and seizures of persons, only a small fraction of which require a warrant); *id.* ch. 8 (discussing searches incident to arrest, virtually none of which require a warrant); *id.* ch. 9 (discussing protective weapons searches and sweeps, none of which require a warrant); *id.* ch. 10 (discussing automobile and consent searches, few if any of which require a warrant); WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT chs. 6-10 (4th ed. 2004) (discussing these same topics).

[63] I do not intend to cite any particular source to defend this statement; anyone who practices criminal law or teaches Criminal Procedure—I've done one or the other for more than forty years—knows it is true (Consider, by analogy, FED. R. EVID. 201(b), which permits a court to take judicial notice of an adjudicative fact that is "generally known within the court's geographic jurisdiction."). Law review editors and judges and attorneys who practice or adjudicate in other areas of law, please keep in mind that the assertion to which this footnote is attached is merely background information in the

lack of probable cause.[64] Probably a more accurate statement would be that as a general rule, warrants based on probable cause *are* required to authorize the police to make a non-consensual entry into a home, office or other private premises; to search someone's mail; to open some packages; and to intercept oral, wire or electronic communications without the consent of a participant.[65]

2. Administrative, Regulatory, and Other "Special Needs" Searches

The government is often called upon to conduct searches in contexts unrelated (or at least not directly related) to criminal law enforcement. These are sometimes referred to as "special needs" searches.[66] The Court has long recognized that the reasonableness of such searches and seizures, conducted outside the traditional criminal law enforcement context, must be measured by standards different from those that apply in criminal cases.[67] The Court has upheld the applicability of this doctrine to inspections of homes[68] and business locations;[69] and to border searches[70] of mail,[71]

---

introductory section of the Article. I respectfully request you simply take my word for its accuracy.

[64] *See supra* note 63.

[65] *See supra* note 63.

[66] *See, e.g.*, City of Ontario v. Quon, 130 S. Ct. 2619, 2628, 2630 (2010) (using the phrase and citing other cases in which it appears).

[67] Each of the cases cited in the next ten footnotes so holds.

[68] *See, e.g.*, Camara v. Mun. Court, 387 U.S. 523 (1967) (holding that a warrant is required before police may search a home pursuant to fire, health, and housing code inspection programs, but that such warrants need not be based on probable cause of criminal wrongdoing or code violations; rather, they may be issued pursuant to reasonable administrative or legislative standards).

[69] *See, e.g.*, New York v. Burger, 482 U.S. 691 (1987) (holding that where a business is closely regulated by the state, searches by the police without a warrant are permissible if carefully limited in time, place, and scope); Marshall v. Barlow's, Inc., 436 U.S. 307 (1978) (holding that a warrant could be issued to search a business location if issued on the basis of a general administrative plan based on neutral principles).

[70] United States v. Ramsey, 431 U.S. 606, 616 (1977) ("That searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border, should, by now, require no extended demonstration.").

automobiles,[72] and individuals;[73] to sobriety checkpoints;[74] and regulations requiring drug tests of school children,[75] law enforcement officials,[76] and mass transit employees.[77] The Court has rejected the application of "special needs" standards with regard to drug interdiction roadblocks,[78] and to regulations

---

[71] *Id.* at 623-24. In *Ramsey*, the Court upheld a statute authorizing customs officials to search first class mail coming from overseas whenever reason existed to suspect it might contain contraband.

[72] United States v. Flores-Montano, 541 U.S. 149 (2004) (upholding border agents' removal, disassembly, and search of a vehicle's gas tank despite the lack of probable cause or reasonable suspicion that it contained contraband).

[73] *See, e.g.*, United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985); Carroll v. United States, 267 U.S. 132, 154 (1925). 19 U.S.C. § 1582 (2006) directs that "all persons coming into the United States from foreign countries shall be liable to detention and search by authorized officers or agents of the Government under such regulations [promulgated by the Secretary of the Treasury]." In *Montoya de Hernandez*, the Court held that where customs agents "reasonably suspect" that a traveler has swallowed contraband in an attempt to smuggle it into the country in her digestive system, the traveler may be detained until the suspicion is verified or dispelled, i.e., until she submits to an X-ray or, if she refuses, until she has a bowel movement. *Montoya de Hernandez*, 473 U.S. at 541.

[74] Mich. Dep't. of State Police v. Sitz, 496 U.S. 444 (1990) (holding that, given the magnitude of the drunk driving problem, sobriety checkpoints that subjected all motorists to a very brief detention was constitutional).

[75] Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995) (upholding a school regulation requiring all students seeking to participate in interscholastic athletics to submit to random drug testing); *see also* Bd. of Educ. v. Earls, 536 U.S. 822 (2002) (upholding a similar regulation regarding all students seeking to participate in any extracurricular activities). In each case the Court held that the school district had documented a serious problem with drug use among children, and that the testing regime was reasonably calculated to help address the problem. In *Safford Unified Sch. Dist. No. 1 v. Redding*, 129 S. Ct. 2633 (2009), however, the Court held that, even though "the [public] school setting 'requires some modification of the level of suspicion of illicit activity needed to justify a search,'" it was unreasonable for an assistant principal who suspected that a thirteen-year-old middle school student possessed over-the-counter pain relief pills to compel the child to submit to a virtual strip search. *Id.* at 2639, 2641-43 (internal citations omitted).

[76] Treasury Emp. Union v. Von Raab, 489 U.S. 656 (1989). See *infra* notes 121-22 and accompanying text for further discussion of *Von Raab*.

[77] Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 611 (1989) (holding that it was reasonable "to require [certain categories of railroad employees] to submit to breath or urine tests" if they were working on a train that was involved in certain kinds of collisions or other incidents).

[78] City of Indianapolis v. Edmond, 531 U.S. 32, 37-38, 40-42 (2000) (The Court held that because such traffic stops (which are Fourth Amendment "seizures") were essentially conducted to enforce criminal laws against drug possession and trafficking, they did not qualify as "special needs" searches and were unlawful absent an individualized suspicion of wrongdoing as to any vehicle that was stopped.).

requiring drug testing for political candidates[79] and for pregnant women seeking free medical treatment at a public hospital.[80]

In 1985, in *New Jersey v. T.L.O.*,[81] a case involving the search of a fourteen-year-old high school freshman,[82] the Court ruled that once it had been determined that a "search" occurred (i.e., that a government agency intruded into a litigant's Fourth Amendment-protected "reasonable expectation of privacy"), the lawfulness of these searches should be assessed by a two-part analysis: "[F]irst, one must consider 'whether the . . . action was justified at its inception,' second, one must determine whether the search as actually conducted 'was reasonably related in scope to the circumstances which justified the interference in the first place.'"[83]

More recently, the Court has applied somewhat differently worded tests in assessing searches in "special needs" situations, even in the absence of individualized suspicion of wrongdoing,[84] and has offered yet another two-part formula for assessing searches generally.[85]

---

[79] Chandler v. Miller, 520 U.S. 305, 319 (1997) (holding unconstitutional a state requirement that all political candidates submit to drug testing because, among other things, the requirement was "not well designed to identify candidates who violate antidrug laws").

[80] In *Ferguson v. Charleston*, 532 U.S. 67 (2001), the Court held that this procedure, done as part of program in which a pregnant woman who tested positive would be threatened with prosecution unless she agreed to submit to treatment, violated the privacy of the women involved because criminal law enforcement was too central an aspect of the program.

[81] New Jersey v. T.L.O., 469 U.S. 325 (1985).

[82] T.L.O. was caught smoking in a bathroom. The assistant principal looked in her purse and saw a pack of cigarettes. When he removed it, he saw cigarette rolling paper, which he associated with marijuana use. At this point, he searched the purse thoroughly and found evidence that the child was selling marijuana to other students at the school. *Id.* at 328.

[83] *Id.* at 341. The Court took this test from, and quoted, *Terry v. Ohio*, 392 U.S. 1 (1968), in which the Court held that a police officer may stop to question someone whom the officer reasonably suspects is committing or is about to commit a crime, and that if the officer reasonably suspects that person is armed, the officer may "frisk" the person (i.e., may run his hands along the outer layer of the person's clothing to see if he is in fact carrying a weapon). *Id.* at 20. In *T.L.O.*, the Court, applying this two-part test, upheld the assistant principal's actions, ruling that each step was justified by what he had discovered by the previous step. *T.L.O.*, 469 U.S. at 347-48.

[84] "In limited circumstances, where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion, a search may be reasonable despite the absence of such suspicion." Skinner v Ry. Labor Execs. Ass'n, 489 U.S. 656, 624 (1989) (quoted approvingly in Chandler v. Miller, 520 U.S. 305, 314 (1997)).

In *Quon*, the Court addressed, but did not decide, whether the *T.L.O.* formula is appropriate when a government agency searches an employee's workspace or his on-the-job communications solely for internal administrative purposes, unconnected with larger government policies or responsibilities. *Quon*, however, was not the first case in which the Court pondered that issue; it had done so twenty-three years earlier, in *O'Connor v. Ortega*.[86] Because an understanding of *O'Connor* is necessary to understand *Quon*, it is to the *O'Connor* case that this Article now turns.

II. *O'CONNOR V. ORTEGA*

A. Facts and Issues

Dr. Magno Ortega had served as Napa State Hospital's Chief of Professional Education for seventeen years.[87] In 1981, Dr. Dennis O'Connor, the hospital's Executive Director, received allegations that Dr. Ortega had engaged in various kinds of wrongdoing.[88] Dr. O'Connor ordered an investigation, during which Dr. Ortega was barred from hospital grounds while hospital officials searched Dr. Ortega's office.[89] The underlying reason for the search was a hotly disputed issue at trial, but in any event, the search was quite thorough: hospital personnel went through his desk drawers and filing cabinets and seized a wide range of objects, including a substantial number of clearly personal items.[90] Dr. Ortega sued the hospital per 42 U.S.C. § 1983,[91] alleging that the search of his office was motivated by a desire to find evidence to support the allegations against him, and therefore violated his Fourth Amendment right against unreasonable searches and seizures.[92] The hospital asserted that the search was conducted to secure state property in the office, and was therefore reasonable.[93] The district court, accepting this defense, granted summary judgment for the hospital.[94] The Ninth Circuit reversed,[95] holding that as a matter of law (1) Dr. Ortega had a reasonable expectation of privacy in his office, desk, and file drawers,[96] and (2) that the search violated that expectation.[97] The Ninth Circuit concluded that the only issue for the trial court to resolve was the amount of damages to which Dr. Ortega was entitled.[98]

---

[85] Wyoming v. Houghton, 526 U.S. 295, 300 (1999) (stating that the reasonableness of a search is determined "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests"). In *Houghton*, the Court upheld a search of all containers in the passenger compartment of an automobile where probable cause existed that at least one occupant possessed a controlled substance. Court quoted and applied the *Houghton* formula in *United States. v. Knights*, 534 U.S. 112, 118-19 (2001), wherein the Court held that a state may legitimately impose, as a condition of probation, that a police officer may search the probationer or his home whenever the officer has a reasonable suspicion that the suspect is engaged in wrongdoing, and in *Samson v. California*, 547 U.S. 843, 848 (2006), where the Court held that a state may legitimately require, as a condition of parole, that a parolee consent to a search whenever asked to do so by a parole officer or law enforcement officer even in the absence of reason to suspect the parolee of any wrongdoing.

[86] O'Connor v. Ortega, 480 U.S. 709 (1987).

[87] *Id.* at 712. Dr. Ortega's primary responsibility was training young physicians in psychiatric residency programs. *Id.*

[88] *Id.* Dr. Ortega was accused of coercing contributions from residents in order to purchase a computer for his office, of sexually harassing two female hospital employees, and of taking inappropriate disciplinary action against a resident. *Id.*

---

[89] *Id.* at 712-13.

[90] *Id.* at 714. These included billing documents of a private patient of Dr. Ortega's. *Id.*

[91] 42 U.S.C. § 1983 (2006) ("Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress . . . .").

[92] *O'Connor*, 480 U.S. at 714.

[93] *Id.* As it turned out, the investigators seized certain items during their searches, but "did not otherwise separate Dr. Ortega's property from state property because, as one investigator testified, '[t]rying to sort State from non-State, it was too much to do, so I gave it up . . . .'" *Id.* at 713-14. No formal inventory was ever made of the contents of the office; "[i]nstead, all the papers in Dr. Ortega's office were merely placed in boxes, and put in storage for Dr. Ortega to retrieve." *Id.* at 714.

[94] Ortega v. O'Connor, No. C-82-4045-JPV, 1993 WL 87804 (N.D. Cal. Mar. 23, 1993) (unreported case).

[95] Ortega v. O'Connor, 764 F.2d 703, 706-07 (9th Cir. 1985), *rev'd sub nom.* O'Connor v. Ortega, 480 U.S. 709 (1987).

[96] *Id.* Concerning the centrality of the "reasonable expectation of privacy" concept to current Fourth Amendment jurisprudence, see *supra* Part I.A.1.

[97] *Ortega*, 764 F.2d at 706-07.

[98] *Id.* at 707.

The hospital appealed and the Supreme Court granted certiorari.[99] Issues before the Supreme Court included: (1) Did Dr. Ortega have a reasonable expectation of privacy in his desk, file drawers, and office? (2) If so, against what standard should that expectation, and the hospital's justification for the search and seizure, be measured? (3) Was the Ninth Circuit correct in ruling that, as a matter of law, Dr. Ortega's right to privacy existed, and that the hospital's actions violated those rights?

In a 5-4 decision, the Supreme Court held that Dr. Ortega indeed did have a Fourth Amendment-protected right to privacy in his desk, file drawers, and office, but concluded that the record below had not been adequately developed to determine whether the hospital's search of his office was reasonable.[100] The Court therefore reversed the Ninth Circuit decision, and remanded.[101] This brief summary of the result, however, is a significant oversimplification. The case produced three separate opinions: Justice O'Connor's plurality opinion (joined by Chief Justice Rehnquist and Justices White and Powell); Justice Scalia's (mostly) concurring opinion;[102] and Justice Blackmun's dissenting opinion[103] (joined by Justices Brennan, Marshall and Stevens).

---

[99] O'Connor v. Ortega, 474 U.S. 1018 (1985) (granting certiorari).

[100] *O'Connor*, 480 U.S. at 727-29.

[101] *Id.* The case has a convoluted history thereafter. After a trial, the judge directed a verdict for the defendants; the Ninth Circuit reversed, ruling the trial judge had improperly precluded Dr. Ortega from calling several witnesses. Ortega v. O'Connor, 50 F.3d 778, 780 (9th Cir. 1995). On retrial, a jury found for Dr. Ortega and awarded him $400,000 in damages; the Ninth Circuit affirmed. Ortega v. O'Connor, 146 F.3d 1149 (9th Cir. 1998). The verdict seems well-justified. During the search, hospital personnel closely scrutinized obviously personal items; the hospital did not permit Dr. Ortega to reclaim his personal property for several months; and it even used some highly private items scrutinized during the search to impeach witnesses who testified on Dr. Ortega's behalf at the post-remand trial. *Id.* at 1152.

[102] Justice Scalia was in the unusual (for him) position of being the swing justice. Of the four issues before the Court, he agreed with Justice O'Connor's plurality on two issues, the Blackmun dissent on one issue, and with neither on yet another issue. *O'Connor*, 480 U.S. at 729 (1987) (Scalia, J., concurring).

[103] *Id.* at 732 (Blackmun, J., dissenting).

B. Reasonable Expectation of Privacy

All nine Justices agreed that Dr. Ortega had a reasonable expectation of privacy in his desk and file drawers.[104] The Court divided, however, as to whether such an expectation existed in his *entire* office. The plurality Justices, after an extensive discussion of the need to consider "[t]he operational realities of the workplace"[105] in order to determine whether an employee's Fourth Amendment rights are implicated by a search of the office as a whole, declined to decide the issue.[106] The four (otherwise) dissenting Justices and Justice Scalia, however, concluded that as a general rule, a government employee *does* have a reasonable expectation of privacy in his or her office. As Justice Scalia put it: "one's personal office is constitutionally protected"[107] except in "unusual situations" in which the office is subject to "unrestricted public access."[108] Thus, a clear 5-4 majority exists as to the office.[109]

---

[104] *Id.* at 718 (plurality opinion); *id.* at 729 (Scalia, J., concurring); *id.* at 732 (Blackmun, J., joined by Brennan, Marshall, Stevens, J.J., concurring with the other five Justices on this issue, although dissenting on pretty much everything else).

[105] *Id.* at 717 (plurality opinion).

[106] *See id.* at 714-18. The plurality declined to decide it, reasoning that the office question was superfluous because the search of his desk and file cabinet clearly had intruded upon Dr. Ortega's reasonable privacy expectations; thus, regardless of how the Court ruled regarding the office, it was necessary for the Court to consider the appropriate standard against which those searches should be measured. *Id.* at 718-19.

[107] *Id.* at 730 (Scalia, J., concurring).

[108] *Id.* at 731.

[109] *Id.* at 732. Despite the unusual source of the five votes on this issue (one concurring Justice and four otherwise dissenting Justices), their conclusion, that Dr. Ortega had a Fourth Amendment-protected expectation of privacy in his office, probably can be considered a "holding" of the Court. In *Marks v. United States*, 430 U.S. 188 (1977), the Court commented: "When a fragmented Court decides a case and no single rationale explaining the result enjoys the assent of five Justices, the holding of the Court may be viewed as that position taken by those Members who concurred in the judgments on the narrowest grounds." *Id.* at 193. (citation omitted) (internal quotation marks omitted). Although the Court certainly "fragmented" in *O'Connor*, the four dissenting and one concurring justices did agree on the rationale for recognizing Dr. Ortega's privacy expectations in his office. *See supra* note 104 and accompanying text.

C. Appropriate Standard to Determine "Reasonableness"

Given the Court's conclusion that Dr. Ortega had a reasonable expectation of privacy in his desk, file drawers, and office, it necessarily follows that when hospital officials examined and boxed up the items they found there, they had conducted a Fourth Amendment "search" of those areas and a Fourth Amendment "seizure" of those items.[110] The Court next addressed the question: What standard should be used to measure the reasonableness of a government employer's search of an employee's private work space? Should a court apply the same standard as the one that police must satisfy when they are seeking evidence of criminal activity, which would generally require a warrant based on probable cause; or a different standard and, if so, what should that standard be?[111]

1. Justice O'Connor's Plurality Opinion

The plurality concluded that the warrant and probable cause requirements should not apply to a search prompted by "special needs," such as a search, like this one, that was based solely on administrative concerns and not possible criminal violations.[112] Justice Scalia agreed.[113] Thus, a 5-4 majority rejected imposing the probable cause and search warrant requirements to "non-criminal" searches by government officials of a government employee's private workspace.[114] Moreover, the plurality and

---

[110] *See supra* Part I.A.1.

[111] The dissent argued that the Court should not have addressed the question at all. *See infra* Part II.C.3.

[112] *O'Connor*, 480 U.S. at 721 (plurality opinion).

[113] *Id.* at 731-32 (Scalia, J., concurring).

[114] Since *O'Connor*, there has been little discussion in opinions of the Court concerning an application of the warrant requirement in non-criminal law contexts. In *Skinner v. Railway Labor Executives Association*, 489 U.S. 602, 611 (1989), the Court held that it was reasonable "to require [specified categories of railroad] employees to submit to breath or urine tests" if a train on which they were working was involved in certain types of accidents or incidents. *Id.* at 611. A six-three majority held that based on the exigencies involved—if blood and urine samples were not taken promptly, the railroad employee's body would eliminate evidence of alcohol or drug use—neither probable cause nor a search warrant was needed. *Id.* at 634. Only Justice Marshall, joined by Justice Brennan, dissented, arguing that while exigencies excused obtaining a warrant before drawing the samples, a warrant should be required before those samples are tested. *Id.* at 642-43.

Justice Scalia explicitly rejected those requirements, whether the search in question was a simple search for a file in the employee's absence, or a search prompted by suspicions that the employee had engaged in wrongdoing. The plurality expressed it thus:

> An employer may have need for correspondence, or a file or report available only in an employee's office while the employee is away from the office. Or, as is alleged to have been the case here, employers may need to safeguard or identify state property or records in an office in connection with a pending investigation into suspected employee misfeasance.[115]

Justice Scalia used the same examples.[116] Thus, a 5-4 majority of the Court decided against applying the warrant and probable cause requirements to a government employer's "special needs" search of an employee's office.

No majority emerged, however, as to what the appropriate standard should be. Justice O'Connor's plurality opinion applied the two-step process that the Court had articulated two years earlier in *New Jersey v. T.L.O*: "[F]irst, one must consider 'whether the . . . action was justified at its inception,' second, one must determine whether the search as actually conducted 'was reasonably related in scope to the circumstances which justified the interference in the first place.'"[117] Given that this two-part test, or similar tests,[118] have been applied in so many other contexts,[119] it may seem sensible enough to apply it as well to government employer-employee searches. But consider: in each of the other cases applying such a formula, the government entity, whether an agency of the federal, state, city, county, or local government, was acting in its capacity *as the government* in the furtherance of *government* goals.[120] Even in *National Treasury*

---

[115] *O'Connor*, 480 U.S. at 721-22 (plurality opinion).

[116] *See id.* at 732 (Scalia, J., concurring) (rejecting the warrant and probable cause requirements for "searches to retrieve work-related materials or to investigate violations of workplace rules").

[117] *Id.* at 726 (quoting New Jersey v. T.L.O., 469 U.S. 325, 341 (1985)); *see supra* note 75 and accompanying text.

[118] *See supra* notes 84-85 and accompanying text.

[119] *See supra* Part I.C.2.

[120] *See supra* Part I.C.2.

Employees Union v. Von Raab,[121] which involved a regulation requiring certain government employees to submit to urine testing, the underlying purpose was not merely the internal administration of the agency, but the broader goal of assuring the honesty and competence of law enforcement officials so they would effectively carry out their public duties.[122]

In *O'Connor v. Ortega*, however, the hospital was *not* acting as a government agency per se; rather, it was acting *strictly* as an *employer* seeking to determine whether one of its employees had misappropriated hospital property or violated hospital policies.

2. Justice Scalia's Concurrence

Justice Scalia, whose concurrence provided the fifth vote rejecting the probable cause and warrant standards, rejected the plurality's two-part formula, protesting that it was so vague as to be almost meaningless.[123] He proposed an alternative: if a government agency searches an employee's workspace while acting solely as an employer, and not in furtherance of any broader governmental function, then the search is lawful so long as the search would be considered reasonable if conducted in a non-governmental workplace. Thus, for example, if the government agency conducts a search "to retrieve work-related materials or to investigate violations of *workplace* rules—searches of the sort that are regarded as reasonable and normal in the private-employer context," then the search is ipso facto reasonable under the Fourth Amendment. [124]

---

[121] 489 U.S. 656 (1989).

[122] In light of the U.S. Customs Service's responsibilities in interdicting and seizing illegal drugs smuggled into the country, the service implemented a program requiring service employees to submit to urinalysis tests if they sought transfer or promotion to positions having a direct involvement in drug interdiction or requiring the incumbent to carry firearms. The Supreme Court upheld the program, concluding that it came within the area of "special government needs beyond the normal need for law enforcement," *id.* at 665-66, i.e., "to deter drug use among those eligible for promotion to sensitive positions within the Service and to prevent the promotion of drug users to those positions." *Id.* at 666.

[123] Justice Scalia objects with some frequency that rules promulgated by the Supreme Court are so vague as to give almost unbridled discretion to judges. See, for example, *Kyllo v. United States*, 533 U.S. 27 (2001), in which the Court, per Justice Scalia, noted criticism of the *Katz* "reasonable expectation of privacy" test as "circular . . . subjective and unpredictable." *Id.* at 34. It was on the same basis that Justice Scalia, in *Crawford v. Washington*, 541 U.S. 36, 62-63 (2004), persuaded the Court to abandon its previous approach to the Sixth Amendment Confrontation Clause and replace it with an entirely different approach (as a result, Confrontation Clause issues are now resolved simply, clearly, concisely, and without the contaminant of judicial subjectivity). To paraphrase Artemus Ward, President Lincoln's favorite humorist, the previous parenthetical "is rote sarcastikul." CHARLES FARRAR BROWNE (ARTEMUS WARD), ARTEMUS WARD: HIS BOOK, A VISIT TO BRIGHAM YOUNG (1862); *see* BARTLETT'S FAMILIAR QUOTATIONS 616:11 (Little, Brown & Co. 15th ed. 1980). For an example of the rather unsettled state of Confrontation Clause law after *Crawford*, see *Michigan v. Bryant*, 131 S. Ct. 1143 (2011).

Although Justice Scalia did not elaborate further, he appears to have reasoned that when a government agency is acting strictly as an employer, and not as a government agency per se, a government employee should enjoy no greater (and no lesser) right to privacy than an employee of a non-government entity. Presumably, therefore, when a government agency conducts a non-criminal-law oriented search, a court should not look to, or create, a body of *Fourth Amendment* law, but should apply *tort and employment law* to determine whether an actionable invasion of privacy has occurred.

3. Dissent

The dissenting Justices accepted the Ninth Circuit's factual conclusion that hospital personnel conducted the search looking for evidence of Dr. Ortega's alleged misconduct, and therefore the search was investigative in nature. Based on this conclusion, the dissent insisted that an *investigative* search of this kind, though it did not involve suspicion of *criminal* conduct, could be lawful only if authorized by a search warrant based on probable cause, albeit with some adjustment of probable cause reflecting the noncriminal nature of the investigation and suspected wrongdoing.[125] Given that the Court remanded the case for further fact-finding, Justice Blackmun also criticized the plurality for "announc[ing] a standard concerning the reasonableness of a public employer's search of the workplace,"[126] adding: "This does not seem to me to be the way to undertake Fourth Amendment analysis, especially in an area[—searches of a government employee's work space—]with which the Court is relatively unfamiliar."[127] He also complained that the plurality's standard was so one-sided that it "makes reasonable almost any workplace search by a public employer."[128]

---

[124] O'Connor v. Ortega, 480 U.S. 707, 733 (1987) (Scalia, J., concurring) (emphasis added).

[125] *Id.* at 732, 741-47 (Blackmun, J., joined Brennan, Marshall and Stevens, J.J., dissenting).

[126] *Id.* at 733.

III. *CITY OF ONTARIO V. QUON*

It was not until the *Quon* decision, twenty-three years after *O'Connor*, that the Court again addressed the issue of government employee privacy.[129] During the interval, lower courts generally considered the *O'Connor* plurality approach to be the applicable law in invasion of privacy suits brought by government employees against their employer.[130] Indeed, in the lower court litigation in *Quon* and in their briefs and arguments before the Supreme Court, both sides in the *Quon* case assumed, federal statutory issues aside, that the *O'Connor* plurality *was* the law.[131]

A. Facts

The facts and lower-court proceedings in *Quon* are fairly complicated. For purposes of this Article, however, the essential facts are these:

1. Jeff Quon was a sergeant in the Ontario Police Department assigned to the SWAT team,[132] presumably a fairly important

---

[127] *Id.*

[128] *Id.* at 734. Despite these concerns, Dr. Ortega ultimately prevailed in his suit. *See supra* note 101.

[129] The Court did address the Fourth Amendment in the Government-as-employer context in *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989), but as noted *supra* note 121-22, that case fell into a "special needs" category of a very different nature than a simple employer-employee relationship.

[130] *See, e.g.*, Ralph V. Seep, Annotation, *Warrantless Search by Government Employer of Employee's Workplace Locker, Desk, or the Like as Violation of Fourth Amendment Privacy Rights—Federal Cases*, 91 A.L.R. FED. 226 (1989 & Supp.).

[131] City of Ontario v. Quon, 130 S. Ct. 2619, 2628 (2010).

[132] *See* BRUCE L. BERG, POLICING IN MODERN SOCIETY 133 (1999) ("Special Weapons and Tactics (SWAT) team[s] . . . [are] squads of specially trained officers [ ] regarded both by citizens and police personnel as elite teams of highly trained and skilled law enforcement agents. . . . Typically, SWAT teams are called to the scenes of ongoing, dangerous situations after more conventional strategies have failed, or when serious and imminent threats to peoples' lives exist . . . . In some jurisdictions, these units simply are called *tactical units*. . . . Members of these tactical teams have received firearms and strategic planning training, as well as training in climbing and

command within the OPD.[133] Each SWAT officer was issued an alphanumeric pager, to enable the officers to communicate with each other if an emergency arose which required their deployment.[134] The city contracted with Arch Wireless Operating Company to provide the wireless services for the pagers.[135] That contract included a set limit of characters per month for each pager.[136]

2. The officers were told officially that they had no reasonable expectation of privacy in any messages they sent or received on the pagers, and that the OPD and the city had the right to monitor or review all messages.[137] This admonition was consistent with the city's previously announced policy, applicable to all city personnel, that the city "reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice," and that "[u]sers should have no expectation of privacy or confidentiality when using these resources."[138] However, OPD Lt. Duke, in charge of the pager system, informally told Sgt. Quon and the others that no one would monitor their messages if they paid for any excess messages (overages) beyond the monthly limit set in the contract between the OPD and Arch Wireless.[139]

3. Sgt. Quon and a few other officers frequently exceeded the limit and paid for the overages.[140] Eventually the OPD Police Chief directed Lt. Duke to obtain two months of text messages sent and received by two officers, including Sgt. Quon.[141] Arch Wireless dutifully provided the transcripts as requested. The parties disagreed as to the reason for the review. Plaintiffs

---

rappelling, handling highjackings and other hostage situations, and riot control tactics.").

[133] *Quon*, 130 S. Ct. at 2624.

[134] *Id.* at 2625.

[135] *Id.*

[136] *Id.*

[137] *Id.* This was communicated to Sgt. Quon and the others verbally and in writing. *Id.*

[138] *Id.*

[139] *Id.* at 2615.

[140] *Id.* at 2625-26.

[141] *Id.* The other officer selected was not a party to the law suit, Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1126 (C.D. Cal. 2006), and the reported decisions in the case do not indicate anything about his messages.

claimed it was to investigate suspicions that Quon was spending too much on-duty time texting on personal matters.[142] Defendants insisted the decision was based on both Lt. Duke's complaints that some of the officers exceeded the limits so regularly that he had essentially become a collection agent for Arch Wireless and on departmental concern that perhaps the monthly character limit included in the contract was too low to cover the officers' on-duty needs.[143]

4. Reviewing Sgt. Quon's messages, Lt. Duke discovered that the overwhelming majority of his messages were not work-related.[144] In fact, Quon was using the pager to exchange sexually explicit messages with his wife Jerilyn, who was also an OPD police officer,[145] and to exchange similar messages with another woman, April Florio, a dispatcher for the OPD with whom he was having an extramarital affair.[146] The matter was referred to the Internal Affairs Bureau of the OPD.[147] An investigator determined that in one month, Quon had sent or received 456 messages during work hours (an average of twenty-eight a day), of which only 10% (an average of three a day) were work-related.[148]

---

[142] *Quon*, 445 F. Supp. 2d at 1144.

[143] *Id.*; *Quon*, 130 S. Ct. at 2626.

[144] *Quon*, 130 S. Ct. at 2626.

[145] *Quon*, 445 F. Supp. 2d at 1122. As the district court described it:

> Many of the text messages sent and/or received by Quon's pager while he was on-duty were, to say the least, sexually explicit in nature. Some of these messages were directed to or from his wife, Jerilyn Quon, while others were directed to or from his mistress, Florio. Other messages, while not sexually explicit were nonetheless private, were sent to and received from his co-worker.

Id. at 1126. This passage gives the distinct impression that Quon exchanged sexually explicit messages with his wife as well as Ms. Florio. However, the Supreme Court's decision in the case refers to "the other respondents, each of whom exchanged text messages with Quon during August and September 2002: Jerilyn Quon, Jeff Quon's then-wife, from whom he was separated . . . ." *Quon*, 130 S. Ct. at 2626. This suggests, albeit not conclusively, that Quon's texts to and from his wife were not sexually explicit.

[146] *Quon*, 445 F. Supp. 2d at 1126. It emerged during a parallel but separate investigation that another OPD dispatcher was tipping off the Hell's Angels motorcycle gang whenever an OPD officer conducted surveillance of a member of the gang, and Ms. Florio was aware of this but did not report it. *Id.* at 1122. Ms. Florio was subsequently fired. *Id.*

[147] *Quon*, 130 S. Ct. at 2626.

[148] *Id.*

5. Sgt. Quon was disciplined for violating OPD rules that forbade pursuing personal matters while on duty.[149]

6. Quon, his wife, and Ms. Florio sued the city, several OPD officials, and Arch Wireless[150] per 42 U.S.C. § 1983,[151] alleging violations of their Fourth Amendment right to privacy, and violations of 18 U.S.C. § 2701, the "Stored Communications Act" (SCA).[152] Sgt. Quon also apparently exchanged numerous non-work-related messages with Sergeant Steve Trujillo, another member of the SWAT team,[153] and Sgt. Trujillo joined as a plaintiff in the suit. The two sergeants and the two women are sometimes referred to collectively as the plaintiffs.[154]

7. The trial judge, attempting to apply the *O'Connor v. Ortega* plurality approach to plaintiffs' Fourth Amendment claim, ruled that the case depended on why the OPD initially decided to review Quon's transcripts—if it was to review the adequacy of the existing contract with Arch Wireless, then the judgment would be for the defendants; if it was to investigate possible wrongdoing by Quon, then judgment would be entered for the plaintiffs.[155] The jury concluded that the Chief of Police ordered the review of officers' text messages to determine whether the character limit on the city's contract with Arch Wireless was sufficient to meet the city's needs. Therefore, the District Court entered judgment for the city and the OPD. The plaintiffs appealed to the Ninth Circuit.

---

[149] *Id.*

[150] This may have made for some fairly interesting plaintiffs' conferences.

[151] *Quon*, 130 S. Ct. at 2626. For the text of 42 U.S.C. § 1983, see *supra* note 91.

[152] For a summary of the SCA, see *supra* Part I.B.2.

[153] None of the court opinions describe the subject of the messages between the two sergeants, which presumably were not as titillating as Quon's texts to and from his wife and Ms. Florio.

[154] Because they were victorious before the Ninth Circuit, the plaintiffs technically were the respondents before the Supreme Court.

[155] The trial judge reasoned that Lt. Duke's informal assurance to the SWAT team members, *see supra* Part III.A., created a reasonable expectation of privacy and concluded that if the review of Quon's messages was investigative, rather than administrative, it violated that expectation. Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1144 (C.D. Cal. 2006).

B. The Technology

An explanation of the technology in question is now in order.[156] Most electronic communications involve one or more Internet service providers (ISPs). Well-known ISPs include G-mail, AOL, Yahoo!, etc. In addition, many companies, private entities like universities, and government agencies are also ISPs, because they provide their own Internet access to employees. When I send an e-mail or text message to a friend, for example, it goes from my computer (or pager or smart phone) to my ISP, whose computer system forwards it to my friend's ISP, which forwards it to my friend's computer or other receiving device. Each ISP must temporarily store the communication within its computer system until its part of the transfer is complete. For example, my friend's ISP retains the message at least until my friend opens it. Moreover, most ISPs retain a back-up copy, more or less indefinitely, even after the recipient deletes it from his or her inbox (Developments in communications technology may soon render this process obsolete, but this is how the Arch Wireless system worked in 2002.).[157] Thus, although Sgt. Quon and those with whom he texted had probably deleted their messages from the devices they were using, Arch Wireless retained copies, and therefore could, and did, provide transcripts of Quon's messages when the OPD asked for them.

C. The Ninth Circuit Decision

On appeal, the Ninth Circuit considered three issues. First, the court considered whether Arch Wireless violated the Stored

---

[156] For a detailed description of how the pager system, including the sending and receiving of text messages, worked, see *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 895-96 (9th Cir. 2008), *rev'd sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619, 2633 (2010).

[157] Sgt. Quon was utilizing a two way alphanumeric pager which enabled him to send and receive text messages to other pagers, e-mail, etc. This same technology is used in cellular phones today. For a brief history of text messaging, see Collette Snowden, *Casting a Powerful Spell: The Evolution of SMS*, in THE CELL PHONE READER: ESSAYS IN SOCIAL TRANSFORMATION 107-24 (Anandam Kavoori & Noah Arceneaux eds., 2006).

Communications Act when it provided the OPD with printouts of the text messages. The Ninth Circuit held that it did.[158]

Second, the Court considered whether Quon and the other plaintiffs had a reasonable expectation of privacy with regard to his non-work related text messages. The Ninth Circuit, attempting to apply the *O'Connor v. Ortega* plurality approach, held that he did.[159] Third, having decided that the plaintiffs had a reasonable expectation of privacy, the court considered whether it was nevertheless reasonable for Lt. Duke to review two months' worth of Quon's text messages. The Ninth Circuit, attempting to apply the *O'Connor* plurality approach, reversed the district court, and held that, as a matter of law, the OPD review was unreasonably intrusive and therefore violated plaintiffs' Fourth Amendment rights.[160]

D. The Supreme Court Decision: Overview

The City of Ontario and Arch Wireless appealed three issues to the Supreme Court: (1) the Ninth Circuit's application of the SCA; (2) the circuit court's conclusion that the plaintiffs had a Fourth Amendment reasonable expectation of privacy in Quon's text messages; and (3) the Ninth Circuit's ruling that OPD's review of those messages constituted an unlawful search of them.

---

[158] *Quon*, 529 F.3d at 903. I believe the Ninth Circuit decided the statutory issue incorrectly. I will not go into detail here, except to note that in holding that Arch Wireless violated the SCA, the Ninth Circuit relied on its earlier decision, *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004). In *Theofel*, defendant Farey-Jones made an unconscionably broad discovery demand upon Theofel's ISP and then improperly exploited the ISP's naïve attempt to comply with it. Theofel sued for damages. Anyone familiar with the facts would want to hit Farey-Jones and his attorney, and hit them hard. The difficulty is that, though their behavior was indefensible, they had not violated either of the federal statutes on which Theofel based his case: the Stored Communications Act and the Computer Fraud and Abuse Act. Faced with this dilemma, the Ninth Circuit proceeded to completely "rewrite" those two statutes to its own satisfaction so Theofel could sue Farey-Jones (For my analysis of *Theofel*, see FISHMAN & MCKENNA, *supra* note 10, § 7:11. If I had the time, I would write an article about that case, whose title would be: "I do not like thee, Theofel. The reason why is plain to tell: you've warped these statutes all to hell! I do not like thee, Theofel.").

[159] *Quon*, 529 F.3d at 904.

[160] *Id.* at 908-09. The Ninth Circuit denied a petition for rehearing en banc. Quon v. Arch Wireless Operating Co., 554 F.3d 769 (2009). Judge Ikuta, joined by six other Circuit Judges, dissented. *Id.* at 774-79. Judge Wardlaw, who voted to deny re-hearing, wrote an opinion responding to Judge Ikuta's dissent. *Id.* at 769-74.

The Supreme Court denied Arch Wireless's cert application on the statutory issue,[161] but granted certiorari on both Fourth Amendment issues.[162]

As it turned out, however, although the Court granted certiorari on the expectation of privacy issue, ultimately, to the disappointment of some and to the relief of others, it did *not* resolve whether Quon had a reasonable expectation of privacy in those text messages.[163] Instead, the Court decided only one issue: the reasonableness of the OPD's review of Sgt. Quon's text messages. Rejecting both the District Court's and the Ninth Circuit's attempts to apply the *O'Connor* plurality approach, the Supreme Court unanimously held that the review of Quon's text messages was reasonable under the circumstances.[164]

But in *Quon*, as in *O'Connor*, unanimity in the result did not lend clarity to the law. A majority of the Court in *Quon*, per Justice Kennedy, explicitly acknowledged that neither the *O'Connor* plurality nor Justice Scalia's *O'Connor* concurrence was firmly established as the law defining how the Fourth Amendment applied to government workplace searches.[165] Justice Kennedy's majority opinion then proceeded to discuss how the *O'Connor* plurality approach might apply to the reasonableness of the review of Quon's text messages.[166] Justice Scalia wrote a somewhat scornful concurring opinion in which he derided the majority's explanation of why it did not decide the expectation of privacy issue,[167] complained that the majority placed too much emphasis on the *O'Connor* plurality approach in addressing the reasonableness of the OPD's review of the text messages,[168] and insisted that his approach to the government workplace privacy issue was and still is the best approach.[169] Justice Stevens, also concurring in the result, argued that neither the *O'Connor* plurality nor the Scalia *O'Connor* concurrence approaches was a good idea, and urged that the Court should eschew any sweeping generalities and decide each case on its facts.[170]

---

[161] USA Mobility Wireless, Inc. v. Quon, 130 S. Ct. 1011 (2009).

[162] *Id.*

[163] The Court's discussion of this issue, and its explanation why it did not decide it, is addressed *infra* Part IV.A.1.

[164] City of Ontario v. Quon, 130 S. Ct. 2619, 2632-33 (2010).

[165] *Id.* at 2628.

[166] This discussion occurs in Part III.B of Justice Kennedy's majority opinion. *Id.* at 2630-32; *see also infra* Part III.E.2.

[167] *Quon*, 130 S. Ct. at 2634-35 (Scalia, J., concurring); *see infra* Part III.F.

[168] *Quon*, 130 S. Ct. at 2635.

[169] *Id.*

E. The Majority Opinion

At the outset, Justice Kennedy, for the Court, reviewed the dispute between the *O'Connor* plurality and Justice Scalia's *O'Connor* concurrence as to the appropriate standard applicable in government-as-employer search cases.[171] The majority then made three assumptions (without deciding those issues) for the sake of its opinion.

1. Three Assumptions

The Court first assumed that Quon had a reasonable expectation of privacy in his non-work-related text messages.[172] Second, the Court assumed that the OPD's review of the message transcripts constituted a Fourth Amendment search. This assumption follows logically from the first because a Fourth

---

[170] *Id.* at 2633-34 (Stevens, J., concurring) (citing O'Connor v. Ortega, 480 U.S. 709, 737-41 (1987) (Blackmun, J., dissenting)). Justices Stevens and Scalia are the only two Justices who had been on the Court when *O'Connor* was decided. They had disagreed in that case and resumed the dispute twenty-three years later in *Quon*. Justice Scalia, in a footnote in his concurrence, accused Justice Stevens of implying that the approach advocated by Justice Blackmun in his dissent in *O'Connor* was still a viable option, and then rejected that implication:

> There is room for reasonable debate as to which of the two approaches advocated by Justices whose votes supported the judgment in *O'Connor*—the plurality's and mine—is controlling under *Marks v. United States*. But unless *O'Connor* is overruled, it is assuredly false that a test that would have produced the *opposite* result in that case is still in the running.

Quon, 130 S. Ct. at 2634 n.* (Scalia, J., concurring). Justice Stevens footnoted back, insisting that the Blackmun approach was not precluded by the Court's decision in *O'Connor*. *Id.* (Stevens, J., concurring). Given that the *Quon* majority paid deference to Justice Scalia's *O'Connor* concurrence while making no reference to Justice Blackmun's *O'Connor* dissent, Justice Scalia wins the footnote battle by a technical knockout, and this Article will not refer further to Justice Stevens's opinion in *Quon*.

[171] *Quon*, 130 S. Ct. at 2629.

[172] *Id.* at 2630. Initially, Quon presumably did not have any such expectation; he was officially told that the OPD reserved the right to monitor messages sent and received. Thus, he would be entitled to a reasonable expectation of privacy only if Lt. Duke created such an expectation when he informally promised not to read Quon's messages so long as Quon paid for any excess over the contracted amount. *See supra* notes 137-39 and accompanying text.

Amendment search occurs when, and only if, a government entity has intruded into a reasonable expectation of privacy.[173] Third, the court assumed that the same principles applicable to a government employer's search of an employee's *physical office* apply as well in the *electronic* sphere.[174]

2. The OPD Review of the Transcripts was Reasonable; Applying the *O'Connor* Plurality Approach

The majority concluded that, even making all these assumptions, the OPD's decision to review Quon's text messages, and the scope and degree of intrusion involved in that review, were reasonable as a matter of law. In explaining this decision, Justice Kennedy, for the Court, stated that it need not decide whether to apply the *O'Connor* plurality approach to privacy in the government workplace, or the approach advocated in Justice Scalia's *O'Connor* concurrence, because the OPD's search in *Quon* was reasonable under either.[175]

Nevertheless, Justice Kennedy's majority opinion proceeded to apply the *O'Connor* plurality approach—first, one must consider whether the action was "justified at its inception," and second, one must determine whether the search as actually conducted was "reasonably related to the objectives of the search and not excessively intrusive in light of the circumstances" which justified the interference in the first place.[176] The Court held that OPD's review of the messages (assuming that this was a "search" at all) was "justified at its inception" because it had a legitimate departmental purpose—to determine whether the monthly character limit was adequate.[177]

The Court also concluded that the manner and intrusiveness of the search were reasonable. First, an examination of the transcripts of Sgt. Quon's transcripts constituted "an efficient and expedient way to determine whether Quon's overages were the result of work-related messaging or personal use."[178]

---

[173] *See supra* Part I.A.1.

[174] *Quon*, 130 S. Ct. at 2629-30; *see infra* Part IV.A.1.

[175] Quon, 130 S. Ct. at 2628-29.

[176] *Id.* at 2630 (quoting O'Connor v. Ortega, 480 U.S. 709, 725-26 (1987)) (internal quotation marks omitted). The Court's application of *O'Connor* to the OPD review of Quon's messages occurs in Part III.B of the Court's opinion.

[177] *Id.* at 2619, 2631 (citations omitted) (citing *O'Connor*, 480 U.S. at 726).

Second, the Court considered the nature and extent of Quon's expectation of privacy in his text messages (assuming he had one at all). The Ninth Circuit apparently concluded that Lt. Duke's promise that no one would audit Quon's messages so long as he paid for the overage gave Quon a nigh-absolute expectation of privacy.[179] Indeed, the only potential diminishment of that right the circuit court mentioned was the possibility that someone might seek Quon's private messages under the California Public Records Act (CPRA), CAL. GOV'T CODE § 6253,[180] a possibility the Ninth Circuit dismissed as so slight as to not be worth considering.[181]

The Supreme Court rejected this reasoning. Assuming Quon *had* a reasonable expectation of privacy in his personal messages, the Court insisted, it is necessary to assess the *degree* to which Quon has a reasonable expectation of privacy in those messages,[182] and the likelihood (from the OPD's viewpoint) that reviewing the transcripts "would intrude on highly private details of Quon's life."[183] The Court concluded that Quon could reasonably expect only limited privacy in his text messages, because as a law enforcement officer, he "would or should have known that his [use of the pager was] likely to come under legal scrutiny" for a variety of legitimate reasons.[184]

---

[178] *Id.* at 2631.

[179] Quon v Arch Wireless Operating Co., 529 F.3d 892, 908-09 (9th Cir. 2008); *see also* Quon v Arch Wireless Operating Co., 554 F.3d 769, 773 (9th Cir. 2009) (Wardlaw, J., concurring in the denial of rehearing en banc).

[180] CAL. GOV'T CODE § 6253 (West 2009), directs that "public records are open to inspection at all times . . . and every person has a right to inspect any public record."

[181] "The CPRA does not diminish an employee's reasonable expectation of privacy [because t]here is no evidence . . . suggesting that CPRA requests to the department are so widespread or frequent" as to deprive OPD personnel of a reasonable expectation of privacy. *Quon*, 529 F.3d at 907 (citations omitted) (internal quotation marks omitted). But consider: suppose there had been no OPD review of Quon's messages, but Mrs. Quon began to suspect that her husband was cheating on her. The thought occurred to her: "Jeff enjoys sexually explicit texting with me. If he has a girlfriend, he probably does the same with her." After consulting with an attorney, she filed a disclosure request per the CPRA. Whither Sgt. Quon's reasonable expectation of privacy then?

[182] *Quon*, 130 S. Ct. at 2631.

[183] *Id.* at 2631.

3. Availability of "Less Intrusive Means"

The Supreme Court was particularly critical of one aspect of the Ninth Circuit's decision in the case. The circuit court, in ruling for the plaintiffs, held that reading Quon's messages was unreasonable because the OPD could have employed several less intrusive means to evaluate the adequacy of the contract with Arch Wireless.[185] The "least intrusive means" concept, and the Supreme Court's treatment of it, merit a somewhat detailed look.

The phrase "least intrusive means" was first used by the Supreme Court in a Fourth Amendment context in *Florida v. Royer*.[186] A plurality of the Court stated that an investigative detention in the absence of probable cause "must be temporary and last no longer than is necessary to effectuate the purpose of the stop," and that "the investigative methods employed should be the *least intrusive* means reasonably available to verify or dispel the officer's suspicion in a short period of time."[187] Since *Royer*, the "least intrusive" principle has been quoted approvingly in an occasional concurring or dissenting opinion.[188] In several decisions prior to *Quon*, however, a clear majority of the Court explicitly rejected the idea that Fourth Amendment searches and seizures were subject to a general "least intrusive means" requirement—in a substantial number of these cases, reversing decisions by the Ninth Circuit in the process.[189] In *Quon*, the Court did so again:

---

[184] *Id.* The Court commented:

> As a law enforcement officer, [Quon] would or should have known that his actions were likely to come under legal scrutiny, and that this might entail an analysis of his on-the-job communications. Under the circumstances, a reasonable employee would be aware that sound management principles might require the audit of messages to determine whether the pager was being appropriately used. Given that the City issued the pagers to Quon and other SWAT Team members in order to help them more quickly respond to crises—and given that Quon had received no assurances of privacy—Quon could have anticipated that it might be necessary for the City to audit pager messages to assess the SWAT Team's performance in particular emergency situations.

Id. The Court did not mention the CPRA.

[185] The Ninth Circuit suggested two such means. First, the OPD could have ordered Quon not to use the pager for personal messages in September; the OPD would thereby obtain an accurate count of the number of characters he used on work-related messages during that month. *Quon*, 529 F.3d at 909. Second, it could have asked Quon to count the characters himself, redact out the personal messages, and permit OPD to review the redacted transcript. *Id.*

[186] Florida v. Royer, 460 U.S. 491 (1983).

[187] *Id.* at 500 (plurality opinion) (emphasis added) (citations omitted). Police officers assigned to airport duty, suspecting that Royer was a drug courier, stopped him and asked him to accompany them to a small police room, retained his ticket and driver's license, and did not inform him that he was free to depart. *Id.* Ultimately the officers

---

searched Royer's luggage and found a significant quantity of marijuana. *Id.* The Court held that the initial stop was reasonable. *Id.* at 501. But the court concluded that the rest of the officers' actions were unreasonable, given that nothing in the record suggested that safety or other legitimate concerns made it inappropriate to question Royer in the open. *Id.* at 501-02 (The Court also upheld a lower court finding that Royer had not consented to the secluded detention. *Id.* at 502-03.). Justice Brennan, whose concurring opinion provided the fifth and decisive vote to suppress the evidence, protested that the plurality opinion constituted a dangerous extension of the stop-and-frisk doctrine promulgated in *Terry v. Ohio*, 392 U.S. 1 (1968), but took some comfort from the plurality's apparent imposition of the least intrusive means limitation on *Terry* stops. Florida v. Royer, 460 U.S. 491, 511 n.* (1983) (Brennan, J., concurring).

[188] *See, e.g.*, Arizona v. Gant, 129 S. Ct. 1710, 1724 (2009) (Scalia, J., concurring); Illinois v. Caballes, 543 U.S. 405 (2005) (Ginsberg, J., dissenting); United States v. Sharpe, 470 U.S. 675, 693-94 (1985) (Marshall, J., concurring).

[189] In *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 663 (1995), the Court reversed the Ninth Circuit and upheld a school system's random urine testing of student athletes without particularized suspicion. *Id.* The Court commented: "We have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment." *Id.* Similarly in another special needs context, see *United States v. Martinez-Fuerte*, 428 U.S. 543, 556-57 (1976), in which the Court, reversing the Ninth Circuit, rejected the "least intrusive means" approach in upholding the constitutionality of permanent immigration checkpoints on major roads near the Mexican border. *Id.* Likewise, see *United States v. Montoya de Hernandez*, 473 U.S. 531, 542-43 (1985), in which the Court reversed the Ninth Circuit's suppression of evidence obtained as a result of a sixteen-hour border detention of a woman suspected (correctly) of attempting to smuggle drugs into the U.S. in her alimentary canal. *Id.* In *United States v. Sokolow*, 490 U.S. 1, 11 (1989), the Court held that, contrary to the Ninth Circuit's view, DEA agents had a reasonable suspicion that Sokolow was a drug courier, and that their temporary detention of him at Honolulu Airport to question him was lawful. *Id.* Stressing that *Royer* was a plurality decision, the Court limited the "least intrusive" principle to

> the length of the investigative stop, not at whether the police had a less intrusive means to verify their suspicions before stopping Royer. The reasonableness of the officer's decision to stop a suspect does not turn on the availability of less intrusive investigatory techniques. Such a rule would unduly hamper the police's ability to make swift, on-the-spot decisions—here, respondent was about to get into a taxicab—and it would require courts to indulge in unrealistic second-guessing."

Sokolow, 490 U.S. at 11 (citations omitted). The Court has rejected arguments based on the "least intrusive" principle in cases from other circuits as well. *See, e.g.*, Bd. of Educ.

> This Court has repeatedly refused to declare that only the least intrusive search practicable can be reasonable under the Fourth Amendment. That rationale could raise insuperable barriers to the exercise of virtually all search-and-seizure powers, because judges engaged in *post hoc* evaluations of government conduct can almost always imagine some alternative means by which the objectives of the government might have been accomplished. The analytic errors of the Court of appeals in this case illustrate the necessity of this principle. Even assuming there were ways that OPD could have performed the search that would have been less intrusive, it does not follow that the search as conducted was unreasonable.[190]

The Court's basic approach to the issue makes good sense and good law. Government officials should not be held to a rigid requirement that, in the absence of probable cause, they must always utilize the procedure that will intrude least into someone's privacy. A "least intrusive" test is equally inappropriate whether the officials are acting in a criminal law enforcement capacity, or in furtherance of "special needs" relating to various public policy concerns, or merely as employers. But the Ninth Circuit did *not* assert that the OPD was required to use the *least* intrusive means to resolve its concerns about Quon's messages and the contract with Arch. Rather, it attempted to apply the second prong of the *O'Connor* test: determining whether the measures adopted were "reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [justification for the intrusion]."[191] The ultimate mandate of the Fourth Amendment is that a search or seizure, to be constitutional, must be "reasonable."[192] The availability of other means, which would achieve the government's legitimate goals while intruding less

---

v. Earls, 536 U.S. 822, 837 (2002) (upholding a school drug testing regime); United States v. Sharpe, 470 U.S. 675, 686-87 (1985) (upholding the twenty-minute detention of a motorist until police could follow up on their suspicions).

[190] City of Ontario v. Quon, 130 S. Ct. 2619, 2632 (2010) (citations omitted) (internal quotation marks omitted).

[191] Quon v Arch Wireless Operating Co., 529 F.3d 892, 908 (9th Cir. 2008) (quoting O'Connor v. Ortega, 480 U.S. 709, 726 (1987)).

[192] Recall that the Fourth Amendment protects "[t]he right of the people to be secure . . . against unreasonable searches and seizures . . . ." U.S. CONST. amend. IV. See *supra* note 9 and accompanying text for the complete text of the amendment.

into someone's privacy, surely is relevant—not an above-all-else factor, but relevant—in assessing the reasonableness of what the government in fact did. The Ninth Circuit cannot be faulted for considering the availability of less intrusive means; its error, rather, was in giving too much weight to them, rather than assessing the overall reasonableness of what the OPD did in light of all the circumstances.

Indeed, the Court in *Quon* implicitly endorsed the principle that, in evaluating the reasonableness of a particular search, a court should consider where that search falls on a spectrum of least intrusive to most intrusive. The Court noted that the police department in fact had conducted its review of Quon's text messages in a way that minimized somewhat the intrusion into his privacy. Although Quon had gone over the character limit during several months, Lt. Duke asked Arch Wireless for only two months' transcripts of Sgt. Quon's text messages.[193] The manner in which the OPD handled the case after Lt. Duke discovered Quon's misfeasance also demonstrates that the OPD took reasonable measures to minimize the intrusion into the privacy of all the plaintiffs. The Internal Affairs investigator assigned to the case read only Quon's on-duty messages, not those Quon sent or received while off-duty.[194] Another point is worth making, although the Court did not mention it: apparently the sexually explicit nature of Quon's text messages with his wife and girlfriend was not disclosed generally within the department. There is no suggestion, in any of the published opinions in the case, that the content of these text messages became general knowledge until, inevitably, they became public as a result of the plaintiffs' law suit.[195]

---

[193] *Quon*, 130 S. Ct. at 2631 ("While it may have been reasonable as well for OPD to review transcripts of all the months in which Quon exceeded his allowance, it was certainly reasonable for OPD to review messages for just two months in order to obtain a large enough sample to decide whether the character limits were efficacious.").

[194] *Id.* at 2631. "[U]sing Quon's time sheets, [the Internal Affairs office] took the transcripts and redacted with a black marker those portions that were transmitted while Quon was off-duty." Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1127 (C.D. Cal 2006). Later Quon's messages with Ms. Florio were examined to see if Quon was in any way involved in the misconduct at the OPD's dispatch center, *see* Part III-A-4, but no such evidence was found. *Id.*

[195] Contrast the behavior of the officers in *Casella v. Borders*, 649 F. Supp. 2d 435 (W.D. Va, 2009). Police seized a cell phone from Ms. Casella's boyfriend, discovered

The Court also stressed that the reasonableness of the OPD's review of Sgt. Quon's messages should also be assessed against what department personnel reasonably *expected* to find. The Court correctly observed that when the OPD undertook to review his messages, his superior officers had no reason to expect that the transcripts would reveal "highly private details" of his life, his wife's, and Ms. Florio's.[196] Although they *did* reveal private details, that was Quon's fault, not the OPD's.

In short, OPD supervisors simply wanted a quick and efficient way to determine whether the characters-per-month package with Arch was adequate. Given all of these circumstances, and the limited privacy expectation (if any) that Quon had in his text messages in the first place,[197] what the department did was quite reasonable, despite the availability of less intrusive (and less efficient) means.[198]

---

that the phone contained sexually explicit photographs of Ms. Casella and her boyfriend, and, allegedly, shared the photographs with dozens of others in and outside the police department. *Id.* at 437. The federal district court dismissed Ms. Casella's § 1983 claim on the ground that even if the seizure of the phone from her boyfriend and subsequent search of the phone violated her boyfriend's rights, there was no violation of her Fourth Amendment rights. *Id.* at 439; *see supra* note 91 and accompanying text. The court pointedly observed that she could still pursue state claims for intentional infliction of emotional distress. *Casella*, 649 F. Supp. 2d at 440.

[196] "From OPD's perspective, the fact that Quon likely had only a limited privacy expectation, with boundaries that we need not here explore, lessened the risk that the review would intrude on highly private details of Quon's life." *Quon*, 130 S. Ct. at 2631. The Court also commented that OPD's audit of Quon's messages on the OPD-supplied pager "was not nearly as intrusive as a search of his personal e-mail account or pager, or a wiretap on his home phone line, would have been." *Id.* This latter observation is of course true, but it is also essentially irrelevant. Because these techniques would not have revealed whether the OPD's contract with Arch was adequate, their use would not have been "justified at [their] inception . . . ." O'Connor v. Ortega, 480 U.S. 709, 726 (1987).

[197] *See supra* note 196 and accompanying text.

[198] It was reasonable for OPD officials to reject the two "less intrusive" methods suggested by the Ninth Circuit, assuming those methods had occurred to them. *See supra* note 185. Ordering Quon not to use the pager for personal messages for a month would have delayed resolution of the OPD's concerns; providing Quon with a transcript of his own messages and relying on him to edit out the personal ones also might have occasioned delays.

4. The Stored Communications Act (SCA) and the Fourth Amendment

Although the Court did not grant certiorari on the statutory issue, it nevertheless discussed the impact of the statute on the constitutional question, and concluded that a federal statute designed to protect privacy plays little or no role in deciding whether a reasonable expectation of privacy exists for purposes of the Fourth Amendment.

Arch Wireless provided Quon's transcripts when asked for them by the OPD.[199] The Ninth Circuit held that Arch violated the SCA by doing so.[200] Although the Supreme Court declined to grant certiorari on that issue,[201] the Ninth Circuit's decision on the SCA provided Quon and the other plaintiffs with a plausible argument: (1) ECPA was enacted to protect the privacy of electronic communications.[202] (2) The SCA, a major component of ECPA, was explicitly enacted to protect the privacy of stored electronic communications, including text messages.[203] (3) The law of the case, based on the Ninth Circuit's decision, is that the OPD obtained copies of Quon's text messages as a result of a violation of the federal statute designed to protect the privacy of such messages.[204] (4) Ergo, in accessing the copies, the OPD unlawfully intruded upon Quon's reasonable expectation of privacy.

The Court gave little credence or attention to this argument:

> [E]ven if the Court of Appeals was correct to conclude that the SCA forbade Arch Wireless from turning over the transcripts, it does not follow that petitioners' actions were unreasonable. Respondents point to no authority for the proposition that the existence of statutory protection

---

[199] *Quon*. 130 S. Ct. at 2626. Arch presumably acted on the assumption that since the pagers were owned by the OPD and that OPD was paying Arch for their use, the OPD had a legal right to the transcripts. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 898 (9th Cir. 2008).

[200] *See supra* Part III.C.

[201] *See supra* Part III.D.

[202] *See supra* Part I.B.2.

[203] *See supra* Part I.B.2.

[204] *See supra* Part III.C.

> renders a search *per se* unreasonable under the Fourth Amendment. And the precedents counsel otherwise.[205]

The Court's almost casual dismissal of the SCA as virtually irrelevant in assessing Fourth Amendment-recognized privacy expectations is disturbing for several reasons. First, the cases the Court cited do not truly support the principle for which they are cited. Second, in *Quon* itself, the Court strongly indicated that *state* statutes may be relevant in determining when expectations of privacy are reasonable. Third, the Court ignored prior precedents relying on federal statutes or regulations in applying the Fourth Amendment.

The precedents the Court cited in this passage do not bear the weight the Court places on them. Each precedent involved the impact of *state* law on the scope of the Fourth Amendment.[206] In each, the Court emphasized the need to have a uniform standard *nation-wide* as to what the Fourth Amendment protected and what it did not.[207] The SCA, however, does not involve state law. It was enacted by the United States Congress and therefore has nation-wide application.

The Court's opinion in *Quon* acknowledged that even *state* statutes may be relevant in determining when an expectation of privacy is reasonable. In explaining why it decided not to decide whether Quon had a reasonable expectation of privacy in his text messages, the Court, discussing society's evolving attitudes about workplace privacy and electronic communications media, cited two state statutes that require employers to notify employees when monitoring their electronic communications.[208]

---

[205] City of Ontario v. Quon, 130 S. Ct. 2619, 2632 (2010) (citing Virginia v. Moore, 553 U.S. 164, 168 (2008)); California v. Greenwood, 486 U.S. 35, 43 (1988)).

[206] *Greenwood* held that a home owner gave up his Fourth Amendment-protected reasonable expectation of privacy in his household garbage when he placed the garbage at the curb for collection, even though California's Supreme Court, applying state law, had previously held that a home owner retained that expectation. *Greenwood*, 486 U.S. at 43. *Moore* held that a search of a motorist incident to his arrest for a traffic violation was reasonable despite a state statute that precluded custodial arrests for mere traffic violations. *Moore*, 553 U.S. at 178.

[207] In *Greenwood*, the Court, by a 7-2 vote, rejected Greenwood's implicit "suggestion that concepts of privacy under the laws of each State are to determine the reach of the Fourth Amendment." *Greenwood*, 486 U.S. at 44. In *Moore*, a unanimous Court, per Justice Scalia, held that the Fourth Amendment was not written to incorporate individual state's arrest statutes. *Moore*, 553 U.S. at 178.

The Court's casual rejection of the SCA as irrelevant to the expectation of privacy issue is inconsistent with its prior considerations of federal legislation when applying the Fourth Amendment. In *United States v. Watson*,[209] the Court, in holding that the Fourth Amendment permitted warrantless arrests for felonies even where the agents had ample time to obtain a warrant, cited several federal statutes that authorize such arrests.[210] In *Florida v. Riley*,[211] a plurality of the Court, holding that no "search" occurred when a police helicopter flew over the defendant's barn at a height of 400 feet to check out a tip concerning marijuana cultivation, relied in part on the fact that although the flight was at a lower altitude than Federal Aviation Commission regulations permitted to fixed-wing aircraft, the flight had not violated that regulation because it did not apply to helicopters.[212] In *Riley*, therefore, the plurality considered a federal regulation not directly related to privacy would be relevant in determining whether a privacy expectation was protected by the Fourth Amendment. If a federal aviation regulation and state statutes are relevant in weighing someone's privacy expectations under the Fourth Amendment, certainly an act of Congress enacted to protect privacy also merits consideration. Moreover, Congress, which is directly elected by and answerable to "society" (i.e., the electorate), presumably reflects, far better than the Supreme Court, what expectations of privacy "society" accepts as reasonable,[213] particularly in an area as challenging and fluid as new electronic communications media.

---

[208] *Quon*, 130 S. Ct. at 2630 (citing Brief for New York Intellectual Property Law Ass'n As Amici Curiae in Support of Respondents, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (08-1332), 2010 WL 1186480, at *22). The Brief in turn cited CONN. GEN. STAT. ANN. § 31-48d (West 2003) and DEL. CODE ANN. tit. 19, § 705 (2005). *See infra* note 271 and accompanying text where these provisions are summarized.

[209] United States v. Watson, 423 U.S. 411 (1976).

[210] *Id.* at 415-16. "Because there is a strong presumption of constitutionality due to an Act of Congress, especially when it turns on what is 'reasonable,' . . . the Court should be reluctant to decide that a search thus authorized by Congress was unreasonable and that the Act was therefore unconstitutional." *Id.* at 416 (quoting United States v. Di Re, 332 U.S. 581, 585 (1948)) (some internal quotation marks omitted). In so holding, the Court reversed a contrary ruling by the Ninth Circuit.

[211] Florida v. Riley, 488 U.S. 445 (1989). Police arranged for a helicopter to fly over Riley's greenhouse. *Id.* Through its partially open roof, the officer observed marijuana plants. Based on this information he obtained a search warrant pursuant to which marijuana was seized. *Id.* at 448-49.

[212] The plurality observed: "We would have a different case if flying at that altitude had been contrary to law or regulation. . . . [I]t is of obvious importance that the helicopter in this case was not violating the law . . . ." *Id.* at 451. The plurality added that it was not saying "that an inspection of the curtilage of a house from an aircraft will always pass muster under the Fourth Amendment simply because the plane is within the navigable airspace specified by law." *Id.* It is worth noting, however, that five Justices (a majority of the Court)—Justice O'Connor, whose concurrence was the deciding vote, and four dissenting Justices—insisted that the reasonableness of Riley's expectation of privacy depended, not on whether the helicopter flight complied with FAA regulations, but on whether helicopter flights at that altitude occurred frequently enough that Riley could reasonably be said to have knowingly exposed the contents of

I do not mean to suggest that Congress should always have the last word on the question. Legislation diminishing an expectation of privacy is properly subjected to a Fourth Amendment challenge. But in enacting the SCA, Congress explicitly *created and protected* an expectation of privacy in communications that are sent and stored by a particular use of technology. Surely the SCA merits greater consideration than the back-of-the-hand the Court gave it in *Quon*.

The Court also rejected petitioners' SCA-based argument on a second, more valid ground. Even if Arch Wireless violated the SCA in turning over the transcripts,[214] this did not involve any wrongdoing by members of the OPD, who reasonably (albeit

---

his barn to the public. *Id.* at 455 (O'Conner, J., concurring). See the dissents of Justice Brennan, who wrote for Justices Marshall and Stevens, and Justice Blackmun. *Id.* at 456, 467 (Brennan, J., dissenting) (Blackmun, J., dissenting). Justice O'Connor joined the plurality opinion because, unlike the four dissenters, she concluded that Riley, not the state, had the burden of proof on the likelihood of such over flights, and had failed to present any (nor had the state). It is worth noting that, under the approach urged by Justice O'Connor and the four dissenters, the result might well depend on where the events occurred. In some parts of the country, at least, low-flying helicopters are a frequent, almost an every-day, occurrence. *See* Adam Nagourney, *Helicopters Jam the Skies over Los Angeles*, N.Y. TIMES, July 25, 2011, at A-1, *available at* http://www.nytimes.com/2011/07/26/us/26choppers.html.

[213] Criticizing the plurality opinion in *O'Connor v. Ortega*, Professor Jeffrey Rosen commented: "It's not surprising that Supreme Court justices, who are secluded in a marble palace and have spent most of their careers in the cosseted solitude of lower courts and universities, aren't terribly good at predicting how much privacy ordinary Americans expect in the workplace." JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 63 (2000).

[214] I consider this a dubious proposition. *See supra* note 158 and accompanying text.

perhaps incorrectly) assumed that the department was entitled to them:

> Furthermore, respondents do not maintain that any OPD employee either violated the law him-or-herself or knew or should have known that Arch Wireless, by turning over the transcript, would have violated the law. The otherwise reasonable search by OPD is not rendered unreasonable by the assumption that Arch Wireless violated the SCA by turning over the transcripts.[215]

Given that this provided the Court with an adequate ground to reject the plaintiffs' SCA-based argument, there was no need for the Court to write so dismissively about the statute, which makes its denigration of the SCA doubly disturbing.

5. Conclusion; Lip Service Deference to Justice Scalia's *O'Connor* Concurrence

Justice Kennedy concluded his lengthy application of the *O'Connor* plurality approach[216] thus: "Because the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable under the approach of the *O'Connor* plurality."[217] His majority opinion then added the following sentence:

> For these same reasons—that the employer had a legitimate reason for the search, and that the search was not excessively intrusive in light of that justification—the Court also concludes that the search would be "regarded as reasonable and normal in the private-employer context" and would satisfy the approach of Justice Scalia's concurrence.[218]

---

[215] City of Ontario v. Quon, 130 S. Ct. 2619, 2632 (2010).

[216] Part III.B of the Court's opinion is 1488 words long (according to the WordPerfect word-counting function), of which almost 1100 words are devoted to the Court's application of the *O'Connor* plurality approach.

[217] *Quon*, 130 S. Ct. at 2632 (citing O'Connor v. Ortega, 480 U.S. 709, 726 (1987)).

[218] *Id.* at 2633 (quoting *O'Connor*, 480 U.S. at 732 (Scalia, J., concurring)).

Part III-B ends thus: "The search was reasonable, and the Court of Appeals erred by holding to the contrary. Petitioners did not violate Quon's Fourth Amendment rights."[219]

F. Justice Scalia's Quon *Concurrence*

Justice Scalia made it quite clear in his concurring opinion[220] that he was not mollified by the majority's passing reference to his *O'Connor* concurrence.[221] First, he asserted his continued conviction that the "operational realities" rubric for determining the Fourth Amendment's application to public employees invented by the plurality in *O'Connor v. Ortega*[222] is standard-less and unsupported. "In this case," he insisted, "the proper threshold inquiry should be not whether the Fourth Amendment applies to messages on *public* employees' employer-issued pagers, but whether it applies *in general* to such messages on employer-issued pagers."[223] This passage in Justice Scalia's concurrence was uncharacteristically poorly drafted. The Fourth Amendment has always been understood to apply only to searches and seizures *by the government or its agents*, not to the conduct of private persons or entities.[224] Presumably what he meant was that "the proper threshold inquiry should be not whether [a reasonable expectation of privacy exists with regard] to messages on *public* employees' employer-issued pagers, but whether [such an expectation exists] *in general* [with regard to] such messages on employer-issued pagers."

---

[219] *Id.*

[220] *Id.* at 2634.

[221] *See supra* Part III.E.5.

[222] *Quon*, 130 S. Ct. at 2634 (Scalia, J., concurring) (quoting O'Connor v. Ortega, 480 U.S. at 717). Referring to this concept, the *Quon* majority commented, "were we to assume that inquiry into 'operational realities' were called for," it would be necessary to determine whether Lt. Duke's informal assurance concerning text messages created an expectation of privacy. *Id.* at 2629 (majority opinion).

[223] *Id.* at 2634 (Scalia, J., concurring) (citations omitted).

[224] Burdeau v. McDowell, 256 U.S. 465 (1921) (holding that the Fourth Amendment, and its exclusionary rule, are "a restraint upon the activities of sovereign authority, and . . . not . . . a limitation upon other than governmental agencies."). They do not, therefore, apply to the acts of "a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." United States v. Jacobsen, 466 U.S. 109, 113 (1984) (citing Walter v. United States, 447 U.S. 649, 662 (1980)). Thus, if someone was acting as an informant at the time he conducted a search, his conduct is measured against Fourth Amendment standards. But if a private person or entity is acting strictly on his, her, or its own initiative, it may turn over the information or evidence thus obtained, and it is admissible at trial even if the private conduct, if it had been done by a government agent, would have violated the defendant's Fourth Amendment rights. *See, e.g.*, *id.*

Second, Justice Scalia wrote, given the Court's unanimous conclusion under both approaches that the OPD's review of Quon's text messages was reasonable, it was unnecessary and misleading for the Court to provide its lengthy application of the *O'Connor* plurality approach. By discussing the *O'Connor* plurality approach at such length, Justice Scalia complained, the Court was hinting, or at least would be perceived as hinting, that this approach was the governing law.[225]

IV. WHAT THE COURT DID NOT DECIDE, AND WHY: EXPECTATIONS AND STANDARDS

Having reviewed what the Court *did* decide, this Article now addresses the more interesting issues: what the Court did *not* decide (including some that were not before the Court). First, against what standard should a government employee's privacy expectations be measured—the *O'Connor* plurality approach, Justice Scalia's approach, or neither—and whether "[t]he principles applicable to a government employer's search of an employee's *physical office* apply with at least the same force when the employer intrudes on the employee's privacy in the *electronic* sphere?"[226] Second, suppose the jury had found, as Quon maintained, that his OPD superiors' real reason for reviewing his text messages was to investigate suspicions of wrongdoing on his part—would the review, as conducted, still be reasonable? Third, can someone who exchanges text messages, e-mail or the like with a government employee have a reasonable expectation of privacy as to those messages, even if the employee does not?

---

[225] *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2635 (2010).

> Despite the Court's insistence that it is agnostic about the proper test, lower courts will likely read the Court's self-described "'instructive'" expatiation on how the *O'Connor* plurality's approach would apply here (if it applied), as a heavy-handed hint about how they should proceed. Litigants will do likewise, using the threshold question whether the Fourth Amendment is even implicated as a basis for bombarding lower courts with arguments about employer policies, how they were communicated, and whether they were authorized, as well as the latest trends in employees' use of electronic media. In short, in saying why it is not saying more, the Court says much more than it should.

Id. (emphasis omitted) (citations omitted).

[226] *Id.* at 2630 (emphasis added).

A. Measuring Expectations of Electronic Privacy

1. The Majority's Waffle: Part III.A of the Court's Opinion

In Part III.A of his majority opinion, Justice Kennedy provided a lengthy explanation of why it *would not decide* whether Quon had a reasonable expectation of privacy.[227] First, Justice Kennedy issued a paean to judicial restraint:

> The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.[228]

His majority opinion then identified the many uncertainties that the issue raised:

> Even if the Court were certain that the *O'Connor* plurality's approach were the right one, the Court would have difficulty predicting how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable. Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their

---

[227] *Id.* Part III.A is nearly 900 words long, of which nearly 800 are devoted to the explanation.

[228] *Id.* at 2629.

> employees, especially to the extent that such policies are clearly communicated.[229]

This passage is significant for several reasons.[230] First, it acknowledges uncertainty as to whether the *O'Connor* plurality approach is the right one.[231] Second, it also recognizes that what happens in the non-governmental workplace will, to some extent, shape what expectations will be reasonable in the government workplace—a concession that appears to be more than just an attempt to mollify Justice Scalia. Third, it acknowledges that no social consensus exists yet as to what privacy expectations might be reasonable in connection with emerging electronic communication media, let alone what expectations might be reasonable concerning their use in the workplace, whether private or governmental. The Court noted that "many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency,"[232] and also noted that at least a few states have enacted statutes that require employers to notify employees concerning when their electronic communications would be monitored.[233]

The pros and cons of the Court's decision not to decide are discussed in Part IV.A.3, *infra*.

---

[229] *Id.* at 2630 (citing O'Connor v. Ortega, 480 U.S. 709, 715) (citations omitted).

[230] Even though the Court decided nothing in this regard, Justice Kennedy's comments on this issue, and Justice Scalia's response, probably garnered more media attention than any other aspect of the case. *See, e.g.*, Orin Kerr, *The Fourth Amendment, New Technologies, and the Case for Caution*, VOLOKH CONSPIRACY (Apr. 20, 2010, 12:40 PM), http://volokh.com/2010/04/20/fourth-amendment-and-new-technologies-and-the-case-for-caution/; *see also*, Adam Liptak, *Justices are Long on Words but Short on Guidance*, N.Y. TIMES, Nov. 18, 2010, at A1, *available at* http://www.nytimes.com/2010/11/18/us/18rulings.html?_r=1.

[231] If five or more of the seven Justices who signed Justice Kennedy's opinion firmly believed that the O'Connor plurality approach was how the law should address these issues, they could have said so.

[232] City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) (citing Brief of Electronic Frontier Foundation, Center for Democracy & Technology et al. as Amici Curiae in Support of Respondents, City of Ontario, California v. Quon, 130 S. Ct. 2619 (2010) (08-1332), 2010 WL 1063463, at *16-20).

[233] *Id.* at 2630 (citing Brief for New York Intellectual Property Law Association As Amici Curiae in Support of Respondents, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (08-1332), 2010 WL 1186480, at *22). The Brief in turn cited DEL. CODE ANN. tit. 19, § 705 (2005), and CONN. GEN. STAT. ANN. § 31-48d (West 2003). See *infra* note 271 for a brief summary of these provisions.

2. Justice Scalia's "I Told You So"

Justice Scalia, in his concurrence, agreed that "there is no need to answer [the] threshold question" about whether the plaintiffs had a constitutional expectation of privacy, because even if they did, the OPD's review of Quon's messages was reasonable.[234] But since no need existed to *decide* that "threshold question," Justice Scalia protested, there was no need for the Court to address it at all.[235] He predicted that the Court's unnecessary discussion of how the *O'Connor* plurality approach might apply to the issue would lead to mischief and confusion among litigators and lower court judges.[236] Moreover, he argued, the majority inadvertently demonstrated the inadequacies of the *O'Connor* plurality formula:

> [I]n fleshing out its fears that applying that test to new technologies will be too hard, the Court underscores the unworkability of that standard. Any rule that requires evaluating whether a given gadget is a "necessary instrumen[t] for self-expression, even self-identification, on top of assessing the degree to which the law's treatment of [workplace norms has] evolve[d]," is (to put it mildly) unlikely to yield objective answers.[237]

Justice Scalia also suggested that the majority exaggerated the difficulties in the question, and acerbically reminded his colleagues that, difficult or not, a case may someday arise that will require that issue to be addressed: "Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice. The-times-they-are-a-changin' is a feeble excuse for disregard of duty."[238]

---

[234] *Quon*, 130 S. Ct. at 2634 (Scalia, J., concurring).

[235] "To whom do we owe an additional explanation for declining to decide an issue, once we have explained that [the issue] makes no difference?" *Id.* at 2635 (Scalia, J., concurring) (emphasis omitted).

[236] *Id.*; *see supra* Part III.F.

[237] *Id.* at 2635 (Scalia. J., concurring) (citations omitted) (quoting *id.* at 2629-30 (majority opinion)).

[238] *Id.* The phrase Justice Scalia used—"the times they are a changin'"—is the title and refrain of a song Bob Dylan wrote in the fall of 1963, which captured the mood of

3. Evaluation; Comparing the Two Approaches

Despite Justice Scalia's scornful criticism, the Court's restraint was probably a good thing, for a variety of reasons. First, it appears from the oral argument that several of the Justices were confused or unclear as to how these pagers worked.[239] For example, some of the Justices may not have been aware that messages were sent through, and stored on, Arch Wireless's computers, rather than going directly from the sender's pager to the recipient's like a phone call.[240] An understanding of this technology would certainly prove useful, if not essential, in analyzing the degree to which privacy expectations in such messages would be reasonable.[241]

Second, at least some prominent scholars worried publicly that a broad decision on the privacy expectation issues in *Quon*

---

many during that troubled and tempestuous period. The basic message of the song is summarized in this verse:

> Come mothers and fathers/ Throughout the land/ And don't criticize/ What you can't understand/ Your sons and your daughters/ Are beyond your command/ Your old road is rapidly agin'/ Please get out of the new one if you can't lend your hand/ For the times they are a-changin'

The Times They Are A-Changin', BOBDYLAN, http://www.bobdylan.com/us/songs/times-they-are-changin (last visited Feb. 28, 2012). For a concise description of the song, its references and significance, see OLIVER TRAGER, KEYS TO THE RAIN: THE DEFINITIVE BOB DYLAN ENCYCLOPEDIA 624-27 (2004).

[239] During oral argument, Chief Justice Roberts asked, "Maybe—maybe everybody else knows this, but what is the difference between the pager and the e-mail?" Transcript of Oral Argument at 29-30, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (No. 28-1332).

[240] During the presentation for the plaintiffs, Chief Justice Roberts asked, "Well, I didn't—I wouldn't think that. I thought, you know, you push a button; it goes right to the other thing." *Id.* at 48. Justice Scalia chimed in: "You mean it doesn't go right to the other thing?" *Id.* Counsel explained: "It's—I mean, it's like with e-mails. When we send an e-mail, that goes through some e-mail provider, whether it be AOL or Yahoo, it's going through some service provider . . . ." *Id.*

[241] Unlike a telephone call, electronic communication technology requires the sender and receiver's ISP's to retain a copy of the contents of an electronic communication at least for a time (The technology is described in Part III.B, *supra*.). ECPA authorizes ISPs to access the contents of customers' messages with no significant restrictions, so long as the ISP does not disclose those contents to others. 18 U.S.C. § 2701(c) (2006); *see also* FISHMAN & MCKENNA, *supra* note 10, § 7:20. Commercial ISPs agree contractually not to do so; otherwise they would lose customers to competitors who do promise to respect their customers' privacy; but when an employer acts as ISP for its employees, it has less motive to make such a promise, and may have valid business or official reasons to monitor certain uses of its equipment and systems.

might put the law into a straightjacket that could cause enormous problems as technology, and society's attitudes toward that technology evolve.[242] As the Court acknowledged, society is still in the process of sorting out how these issues should be addressed.[243]

Justice Scalia's approach—that a government employee's constitutional right to privacy in the workplace should be the same as the legal privacy rights of employees in the private workplace—has its attractions. First, it provides courts with an already existing body of law to apply (assuming that body of law is of sufficient clarity) rather than requiring judges to grope in a vacuum. Second, it avoids creating an artificial distinction which arguably serves no real purpose. Assume two professors' offices and computers are searched by the universities at which they teach, each case involving suspected violations of similar school rules and regulations. Why should a professor at a public university enjoy any greater, lesser, or different right to privacy in her office, than would a professor at a private university? Why should the applicable legal standard be any different? Justice Scalia's approach argues that the standards should be the same.

---

[242] It may be significant that Professor Orin Kerr, who is generally and deservedly acknowledged as one of the nation's leading legal experts on the SCA and on electronic communications generally, wrote several blog entries during the pendency of the case urging the Court not to offer a broad ruling governing expectations of privacy; and that in 2003, Professor Kerr took a leave of absence from George Washington Law School to serve as a law clerk for Justice Kennedy, who wrote the Court's opinion in *Quon*. *See* Orin Kerr, *Communicating With Those Who Have No Privacy Rights: The Hard Question in* City of Ontario v. Quon, VOLOKH CONSPIRACY (Mar. 31, 2010, 1:50 AM), http://volokh.com/2010/03/31/communicating-with-those-who-have-no-privacy-rights-the-hard-question-in-city-of-ontario-v-quon/; Orin Kerr, *Some Thoughts on the Reply Brief in* City of Ontario v. Quon, VOLOKH CONSPIRACY (Apr. 13, 2010, 7:58 PM), http://volokh.com/2010/04/13/some-thoughts-on-the-reply-brief-in-city-of-ontario-v-quon/; Orin Kerr, *Supreme Court Grants Cert on Fourth Amendment Protection in Text Messages*, VOLOKH CONSPIRACY (Dec. 14, 2009, 12:29 PM), http://volokh.com/2009/12/14/supreme-court-grants-cert-on-fourth-amendment-protection-in-text-messages/; Orin Kerr, *The Fourth Amendment, New Technologies, and the Case for Caution*, VOLOKH CONSPIRACY (Apr. 20, 2010, 12:40 PM), http://volokh.com/2010/04/20/fourth-amendment-and-new-technologies-and-the-case-for-caution/; Orin Kerr, *Thoughts on the Oral Argument in City of* Ontario v. Quon, VOLOKH CONSPIRACY (Apr. 19, 2010, 1:44 PM), http://volokh.com/2010/04/19/thoughts-on-the-oral-argument-in-city-of-ontario-v-quon/; Orin Kerr, *Will the Supreme Court Rethink Public Employee Privacy Rights in Quon?*, VOLOKH CONSPIRACY (Dec. 14, 2009, 10:00 PM), http://volokh.com/2009/12/14/will-the-supreme-court-rethink-public-employee-privacy-rights-in-quon/. Other scholars made similar arguments in the lead-up to the Quon decision. *See, e.g.*, Dale Carpenter, *Ninth Circuit Finds Fourth Amendment Protection in Text Messages*, VOLOKH CONSPIRACY (June 18, 2008, 4:39 PM), http://volokh.com/2008/06/18/ninth-circuit-finds-fourth-amendment-protection-in-text-messages/.

[243] *See supra* notes 220-42 and accompanying text; *infra* notes 244-74 and accompanying text.

The question arises: Is there a significant difference between the *O'Connor* plurality approach, and Justice Scalia's tort law, employment law standard?

The common law tort of invasion of privacy is generally divided into four different kinds of wrongdoing: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) publicity placing a person in a false light; and (4) misappropriation of a person's name or likeness.[244] Another tort often associated with these is the intentional, reckless or negligent infliction of emotional damage.[245] The latter four actions are based upon what a defendant did with information once it was obtained; the first, intrusion upon seclusion, is the common law tort that parallels the plaintiffs' claims in *Quon*.

Restatement of Torts, Second § 652B, Intrusion Upon Seclusion, defines that tort as follows: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[246]

Applied to a private sector workplace, to make out a prima facie case for intrusion upon seclusion, a plaintiff must produce evidence sufficient to support a finding that the employer intruded into plaintiff's subjective expectation of privacy; that this expectation was one that society would view as reasonable; that, under the circumstances, society would view the intrusion as highly offensive;[247] and that the employer had no reasonable business justification for the intrusion.[248] In other words, the plaintiff must establish that (1) the employer engaged in a highly offensive intrusion upon the employee's privacy, and that (2) the intrusion was unjustified under the circumstances.[249]

---

[244] RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977); *see also* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 381, 389 (1960).

[245] RESTATEMENT (THIRD) OF TORTS § 45-46 (Tentative Draft No. 5, 2007) (intentional or reckless infliction and negligent infliction).

[246] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[247] Richard E. Kaye, *Cause of Action to Recover Damages for Invasion of Private Sector Employee's Privacy by Intrusion upon Seclusion*, *in* 42 CAUSE OF ACTION 2d 255, §§ 4-5 (West 2009); *see also* L. Camille Hebert, 1 EMP. PRIVACY L. § 8:13 (West 2010) (Employer searches as invasion of privacy: "[A] plaintiff generally is required to establish that the employer committed an unauthorized intrusion into the seclusion of the plaintiff that would be offensive to an ordinary person."). Another useful source may be available in the not-to-distant future. A Westlaw search of the RESTATEMENT

First let us compare the common law tort and the *O'Connor* plurality approach with regard to the nature of the intrusion. The *O'Connor* plurality requires a plaintiff to produce evidence sufficient to support a finding[250] that her government employer intruded into her Fourth Amendment-protected reasonable expectation of privacy; in assessing whether the plaintiff has met this burden, a court must consider "the operational realities of the workplace."[251] This closely parallels the first element of the common law tort action. It is perhaps a bit easier for the public employee to establish the "intrusion" element of her cause of action under the *O'Connor* plurality approach because, unlike the private sector employee, she need not establish that the intrusion

---

(THIRD) OF EMPLOYMENT LAW (database REST-EMPL) for the word "privacy" produces a handful of sections in Chapter 4, each of which promises, "Issues of employee privacy are examined in Chapter 7 of this Restatement." However, accessing the RESTATEMENT's table of contents (by clicking on "table of contents" on the left, about a third of the way down from the top of the screen) reveals that at present the RESTATEMENT consists of only chapters 1-6 and chapter 8. I've been guilty of being tardy with a manuscript or two, so I didn't laugh too loudly when I noticed that.

[248] Kaye, *supra* note 247, § 7. Other defenses, including consent, are discussed in Kaye. *Id.* §6.

[249] *Id.* §§ 4-7.

[250] "Sufficient to support a finding" is the burden of proof a party must satisfy in order to avoid a summary judgment against it at the pleading stage, or a directed verdict at the trial stage. *See, e.g.*, Adickes v. S. H. Kress & Co., 398 U.S. 144, 175-76 (1970) (Blackmun, J., concurring); Law Co., Inc. v. Mohawk Const. & Supply Co., Inc., 577 F.3d 1164, 1170 (10th Cir. 2009); FED. R. CIV. P. 56(c). In *O'Connor*, the trial judge granted summary judgment for the defendants. Ortega v. O'Connor, 764 F.2d 703, 704 (9th Cir. 1985). This amounts to a ruling that, granting all of Dr. Ortega's factual allegations, he had failed to satisfy this burden. The Ninth Circuit reversed, ruling that Dr. Ortega did indeed satisfy his burden of showing an intrusion into his Fourth Amendment-protected privacy and that the defendants failed to satisfy its burden of producing evidence that its conduct was justified. *Id.* at 707. The Ninth Circuit therefore granted summary judgment for Dr. Ortega on the liability issue, and remanded for a trial strictly on the issue of damages. *Id.* The Supreme Court affirmed the Ninth Circuit decision that Dr. Ortega had satisfied his burden of production as to the intrusion, but concluded that a material issue of fact existed as to whether the intrusion was reasonable, and remanded for trial. O'Connor v. Ortega, 480 U.S. 709, 728-29 (1986); see *supra* note 101 for the ultimate disposition of Dr. Ortega's law suit.

[251] *O'Connor*, 480 U.S. at 709-10; *see supra* Part II.B.

was "highly offensive," but unless the intrusion was in fact highly offensive, plaintiff's suit is unlikely to succeed, either as a matter of law,[252] or as a factual issue for the jury.

With regard to the justification issue—here, too, the differences between the two bodies of law, if they exist, appear to be minor at most. If plaintiff satisfies her burden of production as to the intrusion, tort law and the *O'Connor* plurality both place the burden on the employer to establish that the intrusion is justified. Each recognizes that as a general matter, an intrusion is justified if the employer had a valid reason—business[253] or governmental[254]—for it. The *O'Connor* plurality's two-part test adds a bit of flesh to the skeleton, but its two considerations—"first . . . whether the . . . action was justified at its inception," and "second . . . whether the search as actually conducted was reasonably related in scope to the circumstances which justified the interference in the first place"[255]—are just as relevant in the private sector workplace as the governmental workplace.[256]

Each body of law also recognizes an additional defense, besides justification—consent.[257] In the context of electronic communications media, most courts have held that so long as the employer gives the employee specific notice that the employer reserves the right to monitor or review her use of employer-supplied equipment, her use of it constituted implicit consent to the monitoring or review.[258] In this context, as in the law enforcement context,[259] the word "consent," in its everyday meaning, does not accurately reflect reality. "Consent" implies a choice. Here the employee's choice is stark: agree to the employer's policy, or lose the job.[260]

---

[252] If the plaintiff establishes only that her government employer made only a minor intrusion into her privacy, the agency will not have to establish much of a justification for it to be entitled to judgment as a matter of law.

[253] Kaye, *supra* note 247, § 7.

[254] *See infra* note 255-56 and accompanying text.

[255] *O'Connor*, 480 U.S. at 726; *see supra* Part II.B.

[256] "[T]he sufficiency of an employer's business justification for intruding on employees' privacy is a function of (1) the validity and veracity of the economic or health/safety rationales for the intrusion; and (2) whether the means or methods used were proportionate to the employer's purported justification for the intrusion." Kaye, *supra* note 247, § 7; *see id.* §§ 8-24 (reviewing the law as it applies to a variety of information-gathering techniques and the justifications asserted by employers).

[257] Concerning the private sector workplace, see Kaye *supra* note 247, § 6. Concerning consent generally as a defense to civil or criminal charges of unlawful electronic surveillance, see FISHMAN & MCKENNA, *supra* note 10, §§ 5:101-5:107.

[258] FISHMAN & MCKENNA, *supra* note 10, § 6:5.

[259] *See supra* Part I.A.2.

Many government agencies and private sector employers now require employees to sign a statement acknowledging that they have no reasonable expectation of privacy in their use of the employer's communications equipment and systems.[261] If an employer asked my advice on this matter, I would recommend that every employee be required to sign such a statement,[262] and would also advise the client to order supervisory personnel not to make any "informal" or "off-the-record" assurances to the contrary.[263] The odds are that this practice is, or soon will become, so pervasive and routine that employees are unlikely to have grounds to sue either a government employer based on the Fourth Amendment, or a private sector employer based on intrusion upon seclusion.[264] Such suits are likely to arise only against small, unsophisticated employers, and in cases where, like *Quon*, a supervisor gives employees "unofficial" or "off-the-record" assurances that, despite the official policy, no monitoring or review will be conducted.[265]

---

[260] *See, e.g.*, Frye v. IBP, Inc., 15 F. Supp. 2d 1032, 1041-42 (D. Kan. 1998) (holding that an employee's submission of a urine sample, in compliance with his employer's drug testing policy, constituted consent and therefore a defense under RESTATEMENT (SECOND) § 652B (2011), even though his refusal would have cost him his job).

[261] *See generally* WILLIAM S. HUBBARD, THE NEW BATTLE OVER WORKPLACE PRIVACY ch. 7 (1998); MICHAEL R. OVERLY, E-POLICY: HOW TO DEVELOP COMPUTER, E-MAIL, AND INTERNET GUIDELINES TO PROTECT YOUR COMPANY AND ITS ASSETS (1999).

[262] For examples of such statements, see the books cited in the previous note.

[263] I would also advise the client: (1) not to monitor or review an employee's use of the equipment unless a good business reason presented itself; (2) where the need arises, monitor or review in a way that minimizes the intrusion into the employee's privacy to the extent reasonably practicable; (3) restrict dissemination of the information obtained to those with a clear need to know; and (4) use the information as discreetly as possible.

[264] If the employer makes inappropriate disclosure or use of the information obtained from the monitoring or review, this may give the employee a cause of action for example for public disclosure of private facts, false light, etc. *See supra* notes 244-46 and accompanying text.

[265] It is easy to understand what motivated Lt. Duke to give his informal assurance to the members of the OPD SWAT team. *See supra* notes 137-39 and accompanying text. He had no desire to snoop on the members of the SWAT team, and saw no harm in reassuring them of that. But if he had not made his informal reassurances, perhaps Quon would have been more discrete in his use of the pager; and if not, in all likelihood the district court and Ninth Circuit would have dismissed the plaintiffs' law suit on the

4. The Need for Legislation

Given that the *O'Connor* plurality approach and the common law regarding right to privacy in the workplace so closely resemble each other, does it really matter which ultimately becomes the law governing privacy in the governmental workplace?

I believe it does. To assess the Fourth Amendment reasonableness of government conduct solely by what is done by employers in non-government workplaces would be an abdication of the government's and (at least, in the absence of congressional legislation the Supreme Court's) responsibility to determine what intrusions by the *government* into individual privacy are reasonable. As Justice Brandeis famously admonished eight decades ago, "[o]ur government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example."[266] The *Quon* majority recognized that it would be wrong for the Court to ignore what is happening in the non-government workplace,[267] but there is merit to the proposition, implicit in the *O'Connor* plurality approach, that the Fourth Amendment should not blindly follow the practices of the private sector. This is particularly so given that, regarding workplace privacy (among other employment matters), private employers often can pretty much set whatever rules they please, because workers lack the individual or collective power to object.[268]

---

ground that Quon, and those with whom he texted, had no reasonable expectation of privacy in the first place.

[266] Olmstead v. United States, 277 U.S. 438, 485 (1928) (Brandeis, J., dissenting) (protesting the admission at trial of evidence obtained by unlawful wiretaps by federal agents).

[267] City of Ontario v. Quon, 130 S. Ct. 2619, 2629-30 (2010).

[268] Federal and state law do protect workers in many fundamental ways, but from what experts in the field tell me, there is no explicit body of labor law legislation that addresses these issues. Labor unions can insist on some degree of protection of worker privacy, but can do so only in industries that are heavily unionized, and in recent decades, unions have represented a shrinking portion of the labor market. According to the Census Bureau's Statistical Abstract of the United States 2011, in 1985, nearly 17 million workers were union members and more than 19 million were covered by union contracts—18% and 20% of the labor market respectively; by 2009 those numbers had diminished to 15 million and 16.9 million (12.3% and 13.6%). This decline is even more noteworthy considering that the nation's population grew by roughly 70 million people during the intervening quarter century. Moreover, while in 1985, nearly two-thirds of those whose jobs were covered by unions were private sector workers, by 2009 less than

According to data collected by the American Management Association (AMA), private sector employers are monitoring their employees more than ever before. According to the AMA's 2007 Electronic Monitoring & Surveillance Survey, 66% of employers monitor their employees' Internet connections, 65% of companies use software to block connections to inappropriate Web sites, 43% of companies monitor e-mail, 45% monitor time spent on the telephone and numbers called, 16% record phone conversations, and almost half (48%) of the companies surveyed use video monitoring to counter theft, violence, and sabotage.[269]

Given these complexities, defining privacy expectations should be the responsibility of Congress, not the Court.[270] Legislative models exist from which Congress could construct a reasonable regime. As the Court noted in *Quon*, at least two state statutes require employers to notify employees in advance if they plan to monitor or review employees' use of employer-provided communications equipment, or if it reserves the right to do so.[271]

---

half were private sector workers—a total of 8.2 million. Given that fewer workers in the private sector are in industries with a strong union presence, most private sector workers will have little leverage to bargain for greater privacy. The labor statistics in this footnote are found in the CENSUS BUREAU STATISTICAL ABSTRACT 429 tbl. 663. The population figures for 1985 and 2009 may be found at *Population Estimates: Historical Data*, U.S. CENSUS BUREAU, http://www.census.gov/popest/national/national.html (last visited Feb. 21, 2012).

[269] Kaye, *supra* note 247, at 290. According to the AMA, of the 304 U.S. companies that participated in the survey: 27% represent companies employing 100 or fewer workers, 101-500 employees (27%), 501-1000 (12%), 1001-2500 (12%), 2501-5000 (10%), and 5001 or more (12%). AM. MGMT. ASS'N, 2007 ELECTRONIC MONITORING AND SURVEILLANCE SURVEY 12 (2008), *available at* http://www.amanet.org/download.aspx?filename=%2fimages%2felectronic-monitoring-surveillance-survey08.pdf&pid=41.

[270] I write this sentence assuming that Congress will somehow find the time to devote to anything other than not resolving the nation's debt ceiling and fiscal crises (I originally wrote the preceding sentence in late July 2011, as the fiscal apocalypse (defaulting on the nation's debt) drew nigh. In light of the temporary, jury-rigged "compromise" that was ultimately struck, I see no reason to revise it.).

[271] *Quon*, 130 S. Ct. at 2630 (citing CONN. GEN. STAT. § 31-48d (2003); DEL. CODE ANN. tit. 19, § 705 (West 2005)). Each statute requires advance written or electronic notice to the employee. CONN. GEN. STAT. 31-48d(b) (2003); DEL. CODE ANN. tit. 19, § 705(b) (West 2005). Each authorizes a state agency to impose a civil penalty on an employer who fails to comply with the provision. CONN. GEN. STAT. § 31-48f (2003); DEL. CODE ANN. tit. 19, § 705(d) (West 2005) (specifying in the latter provision that the civil penalty is not an exclusive remedy and does not preclude a suit for damages under any other state or federal law). Each statute contains exceptions where the monitoring or review is conducted in cooperation with law enforcement officials. CONN. GEN. STAT. § 31-48d(d) (2003); DEL. CODE ANN. tit. 19, § 705(b) (West 2005).

Many (perhaps most) federal agencies already provide such notice; Congress should make this mandatory. Beyond this basic step, consider the federal statute that regulates the interception of telephone calls. Although Title III is not a model of clarity in this regard, in essence it permits employers (whether in the private or governmental sectors) to surreptitiously monitor an employee's phone conversations only if, and to the extent, that it has a valid business purpose to do so. Excessive monitoring violates the statute and therefore is civilly actionable.[272] A similar regime would serve as well with regard to electronic communications, including e-mails, text messages, and the like.[273]

The federal government has attempted to encourage and inspire states and private entities to emulate it in a variety of contexts.[274] It is plausible to argue that, with regard to workplace privacy, Congress should take the initiative to set an example that enlightened non-government employers might choose to follow. Until it does, the *O'Connor* plurality approach to the issue, for all its vagueness and other shortcomings, is preferable to Justice Scalia's.

---

[272] The preceding sentence is a very brief summation of a somewhat complex subject. *See* FISHMAN & MCKENNA, *supra* note 10, §§ 6:3-6:13. Moreover, an employer may deprive employees of this protection merely by informing them that all calls may be monitored. As a general rule, an employee who uses a phone while on notice that it may be monitored is deemed to have consented to the monitoring. *See id.* § 6:5.

[273] Even if such a statute was enacted applying this approach to electronic communications media generally, and was made applicable to the private sector as well as to the government, employers could frustrate such a statute by requiring employees to sign an acknowledgement that they have no expectation of privacy when they use employer-supplied communications media. Even so, such a statute might have the aspirational impact of encouraging employers to act reasonably with regard to employee privacy.

[274] See, for example, Exec. Order No. 13,514, 3 C.F.R. § 248 (2009), on Federal Leadership in Environmental, Energy, and Economic Performance, setting forth the administration's plan to lead by example in the area of energy conservation and environmentally sensitive operations. Similarly, see the Telework Enhancement Act of 2010, 5 U.S.C. §§ 6501-06 (2010), setting forth the government's policy for allowing federal employees to telecommute and encouraging the private sector to do the same. *See* Steve Vogel, *Report Urges U.S. Government To Boost Workplace Flexibility*, WASH. POST (May 14, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/05/13/AR2009051303688.html (relating that a government report that led to the enactment of that statute urged the federal government to "lead by example" by including flexible work arrangements).

B. Suppose the Jury Had Found That the Review Was to Investigate Suspicions of Quon's Wrongdoing

At trial, the plaintiffs claimed that the real reason OPD personnel reviewed Sgt. Quon's text transcripts was to investigate suspicions of wrongdoing on his part, but the jury found that the review was motivated only by concerns over the adequacy of the OPD's contract with Arch.[275] Cases no doubt have arisen or will arise, however, in which an agency monitors or examines an employee's use of government-provided electronic communication equipment to investigate possible wrongdoing. Thus, it is worth considering how this might have affected the Court's resolution of the issues in *Quon*.

At first glance, the answer might be: not at all. In *O'Connor*, after all, the plurality opinion and Justice Scalia's concurrence each emphasized that their approaches applied whether the agency's search was for a needed file, or to investigate suspicions of employee wrongdoing.[276] In the latter situation, depending on what the employee is suspected of doing, the agency's need to act quickly might be more compelling than existed in *Quon*.[277] On the other hand, where the employee is suspected only of occasional use of the equipment to send and receive personal messages while on duty, the need for immediate action by the agency is less compelling. The agency, moreover, would have reason to suspect that the monitoring or review would reveal some personal details of the employee's life. In *Quon*, the Court, in upholding the reasonableness of the OPD's review of Quon's text messages, stressed that at the outset the OPD did *not* anticipate that the messages would include highly personal information.[278]

Given the unique facts in *Quon*—that he was told officially that he had no expectation of privacy in the messages; that he was given only informal assurances to the contrary; and that the nature of his job made it likely that some of his messages, at any rate, might become relevant evidence if a SWAT team action ever lead to litigation—I suspect the Court would have held that the

---

[275] *See supra* note 155 and accompanying text.

[276] *See supra* Part II.C.1 (plurality opinion) and II.C.2 (Justice Scalia's concurrence).

[277] Such would be the case, for example, if the employee was suspected of using the device to harass other individuals or reveal confidential information to outsiders.

[278] *See supra* Part III.E.2.

OPD's review of Quon's messages was reasonable even if the jury *had* concluded that the OPD reviewed Quon's messages to investigate suspicions that he was engaging in some kind of misfeasance. But professorial speculation is small comfort to public officials who must make on-the-spot decisions.

C. Privacy Expectations of Those With Whom Quon Texted

Given, as the Court unanimously agreed, that OPD's review of Sgt. Quon's text messages did not violate his Fourth Amendment rights, the question remained: did it violate the rights of the other plaintiffs? In Part III.C of the majority opinion, the Court acknowledged this issue, noting that the plaintiffs and defendants "disagree[d] whether a sender of a text message can have a reasonable expectation of privacy in a message he knowingly sends to someone's employer-provided pager."[279] It was not necessary for the Court to address that issue, however, because the other plaintiffs based their case solely on the theory that the OPD review violated Sgt. Quon's rights and, derivatively, their own.[280] Once the Court rejected Sgt. Quon's Fourth Amendment case, the other plaintiffs' claims also fell.[281]

The Court's refusal to discuss the issue was correct given the facts, and, given the facts, it is easy to assume that the other plaintiffs did not press any claims independent of Sgt. Quon's because they all knew Sgt. Quon was using a pager issued by the OPD. This aspect of the case would have been far more interesting if one of Sgt. Quon's text-correspondents did *not* know that the sergeant was using an OPD device to send and receive the messages.

Suppose, for example, a police department (PD) provided an officer with a pager, or a cell phone with text messaging ability, for use on official business. The officer used it to exchange sexually explicit messages with a woman who was not an employee of the PD and was unaware that the officer was using a device issued to him by the PD. [282] After awhile, the PD decided, for legitimate departmental reasons, to review the officer's text messages, and did so in a reasonable manner, and thereby discovered the contents of the officer's and the woman's messages. The officer would have no Fourth Amendment claim against the PD for a variety of reasons.[283] Might the woman have a Fourth Amendment claim against the department, independent of the officer's?

---

[279] City of Ontario v. Quon, 130 S. Ct. 2619, 2633 (2010).

[280] *Id.* In fact, all four plaintiffs (Quon, his wife, his girlfriend, and Sgt. Trujillo) were represented by the same attorney before the Court.

[281] *Id.* On this point, the Court was unanimous—neither Justice Scalia nor Justice Stevens commented on this aspect of the decision.

At first blush, the answer is clearly no—if it was reasonable for the PD to review the text messages the officer sent and received, it logically follows that both sides of each exchange come within the scope of the review. This follows the approach the law applies to the surreptitious *interception* of communications authorized by Title III: if the authorities obtain a lawful tap or bug and execute it lawfully, the intercepted communications are admissible against each participant—those named in the application and intercept order, and also those, originally unknown, who are overheard engaging in crime-related conversations.[284] This logic arguably applies with equal force to an after-the-fact review of an employee's messages lawfully conducted pursuant to the Fourth Amendment's special needs doctrine—Or does it?

Title III authorizes the *surreptitious* interception of a suspect's wire, oral, or electronic communications, because the interception must be surreptitious if the government is to have any realistic chance of achieving its authorized goals—common sense suggests that a criminal will not plan or discuss his criminal activities over a phone that he knows is tapped or in a premises that he knows is bugged.[285] Often, the officers reasonably expect, or learn as the investigation progresses, that many, even most, of those with whom the initial targets converse are also engaged in crime. Moreover, an interception order authorizes the interception only of communications relevant to the crimes under investigation; if the police learn that a particular individual is not involved in criminal activity, they must "minimize" the interception of his or her conversations.[286]

---

[282] I am using this gender line-up in my hypothetical for convenience, and to parallel the facts in *Quon*. I acknowledge, of course, that the roles might be reversed—she might be the police officer and he might be the civilian; or they could both be of the same gender.

[283] If he had been informed that he had no reasonable expectation of privacy in his messages, and that the PD reserved the right to review them, that would be enough to deprive him of Fourth Amendment protection. Even if he did have some right to privacy, it presumably would be limited for the reasons the Court discussed in *Quon*. *See supra* Part III.E.2. Finally, even assuming he had some reasonable expectation of privacy, if the PD had a valid reason to review those messages and did so in a reasonable manner, although its review would intrude into his privacy, it would not violate it.

[284] *See generally* FISHMAN & MCKENNA, *supra* note 10, §§ 8:27-8:34.

None of these circumstances, assumptions, or restrictions would apply to the woman in my hypothetical. Unlike the person who meets with, calls, or receives calls from a suspected drug dealer whose office is bugged or whose phone is tapped, there is no basis to assume that she is engaged in any wrongdoing.[287] More important, the PD has no compelling reason to avoid informing those with whom the officer texts, that he is using a PD device and the messages are subject to PD review.[288] Indeed, serving such notice would *enhance* the PD's interests, because it would

---

[285] Common sense is not always an accurate predictor of how people actually behave. Prison and jail inmates and those with whom they converse are on notice that their phone calls will be monitored or recorded, as will their face-to-face visits. Despite these warnings, many prisoners do use prison phones or face-to-face visits to discuss or plan crimes, and recordings of those conversations are routinely admitted into evidence against the participants in the conversations . . . (Perhaps these prisoners and those with whom they converse are not very bright, or perhaps they have a remarkable facility for denying reality, or are simply too bored to care.). For a discussion of the various legal theories justifying this result, see FISHMAN & MCKENNA, *supra* note 10, §§ 6:42-6:57; admissibility of the recordings against the non-prisoner participant is discussed *id.* §§ 6:51 (phone calls) and §§ 6:53-6:54 (oral communications during prison visits).

[286] Title 18 U.S.C. §2518(5) (2006) requires each interception order to contain a directive "that the authorization to intercept . . . shall be conducted in such a way as to minimize the interception of communications not otherwise" relevant to the investigation. It is universally acknowledged, of course, that even under the best of circumstances, some irrelevant conversations will be intercepted and recorded, including many involving people not engaged in criminal activity. For a detailed discussion of the "minimization clause," see FISHMAN & MCKENNA, *supra* note 10, §§ 8:101-8:107. For a discussion of how law enforcement officials should attempt to comply with the minimization provision, see *id.* ch. 15. For a discussion of the issues that arise at a pretrial "minimization hearing," see *id.* §§ 35:50-35:74.

[287] If she is aware that the officer is married, her conduct in exchanging sexually explicit text messages with him is immoral, but of itself, that is no business of the PD's, and she should not thereby forfeit an otherwise protected expectation of privacy.

[288] Obviously exceptions exist, such as where the officer is acting "under cover" of a different identity for investigative purposes.

(presumably) discourage others from sending personal messages to that device.

As a rule, whenever we make or receive a phone call, or send or receive an e-mail or text message, we assume that its privacy is legally and technologically protected. Those of us who are knowledgeable about the law or communications technology are aware that there are many ways in which that privacy may be breached;[289] but in general, the only real risk is that the person with whom we are communicating will share what was said with others.[290]

There are, of course, situations in which this assumption is not justified, but usually we are given notice. Many private companies and public agencies provide such notice on their telephone lines: after dialing a company or agency number, we have all heard messages advising us that the call might be "monitored for quality control purposes" or the like.[291] Similarly, many government agencies (and perhaps some companies) automatically include in each outgoing e-mail a notice to this effect,[292] or at least an advisory to examine the agency or company's privacy statement on its Web site.[293]

---

[289] Some of the legal means are discussed *supra* Parts I.A.2 and I.B.

[290] Each of us has from time to time been the victim of a betrayal of confidentiality; each of us has committed such a breach. A few decades ago, the betrayals were generally limited to the immediate acquaintances of those concerned. One of the dubious blessings of the Internet is that it is now possible for a betrayed confidence to circulate among thousands and even millions of strangers. *See, e.g.*, T.R. Reid, *Thanks for Last Night! (cc: The Entire World)*, WASH. POST, Dec. 18, 2000, at C1.

[291] This experience is becoming less and less frequent as companies and agencies switch to automated phone answering systems ("Please make a selection from the following menu. To start a new subscription, press 1 . . .") designed to prevent a caller from ever speaking to a human being.

[292] Florida's may be the most all-encompassing in this regard. FLA. STAT. ANN. § 119.01 (West 2012) provides, in pertinent part:

> (1) It is the policy of this state that all state, county, and municipal records are open for personal inspection and copying by any person. Providing access to public records is a duty of each agency.
>
> (2)(a) Automation of public records must not erode the right of access to those records. As each agency increases its use of and dependence on electronic recordkeeping, each agency must provide reasonable public access to records electronically maintained and must ensure that exempt or confidential records are not disclosed except as otherwise permitted by law.

Given all this, the woman in our hypothetical has a plausible argument that the failure to provide her with notice[294] falsely created the impression that her messages with the officer enjoyed the usual degree of privacy enjoyed by private text messages between two individuals; and that the absence of such notice means that the PD intruded upon *her* Fourth Amendment-protected reasonable expectations of privacy, even if it did not intrude upon the officer's.

Including such a notice in all outgoing e-mail and text messages would not completely protect outsiders from the risk that a nondescript e-mail address or phone number is actually a government or corporate device. If I exchange phone numbers with woman at a social event and decide to send her a rather personal text message describing the powerful impression she made on me and how her image haunts my dreams and fantasies,[295] I may have no way of knowing that the number to which I am texting is her FBI-issued smart phone; that realization would come only when I receive her reply, with privacy notice included. If for some reason her superiors at the Bureau are monitoring her text messages and therefore read what I sent her,

---

> (b) When designing or acquiring an electronic recordkeeping system, an agency must consider whether such system is capable of providing data in some common format . . .

I have corresponded with a police officer in Florida. The following appears at the end of each of his e-mails:

> PLEASE NOTE: Florida has a very broad public records law (F. S. 119). All e-mails to and from County Officials are kept as a public record. Your e-mail communications, including your e-mail address may be disclosed to the public and media at any time.

Incidentally, the officer informs me that this notice does not appear in each text message he sends.

[293] Even in the absence of such notice, common sense should warn us that when we receive an e-mail from or send an email to firstname.lastname@megacorp.com or Jeff.Quon@OntarioPD.gov, given the corporate or governmental nature of the entity involved, the possibility exists that someone in addition to the named recipient may read what we send.

[294] Such notice need not be elaborate or lengthy. The shortest I've been able to come up with is: "Official use only. See www.OPD.city/privacy," which consists of forty characters.

[295] This situation is entirely hypothetical. I have been happily married for more than forty-three years—without interruption, and to the same woman. *See supra* note 59.

well, tough luck on me. Government entities and private employers are not required to do everything conceivably possible to protect the privacy of those who communicate with their employees;[296] they should only be required to act reasonably. But it places no great burden on employers to include a brief notice about the lack of privacy in all outgoing e-mails, text messages and the like. Failure to do so might reasonably be held to create an expectation of privacy.

CONCLUSION

In *City of Ontario v. Quon*, the Supreme Court could have clarified many aspects of the law concerning (1) a government employee's claim that his employer improperly intruded upon his Fourth Amendment-protected reasonable expectation of privacy, and (2) the applicability of the Fourth Amendment to an employee's use of employer-supplied electronic communications equipment. It chose to resolve neither of these issues. In fact, it left the law more unsettled than it had been.

As to the first issue, prior to *Quon*, it had been generally understood that the plurality opinion in *O'Connor v. Ortega* was in fact the law.[297] In *Quon*, however, the majority explicitly declined to endorse this view, instead pointing out that the *O'Connor* plurality approach did not capture a majority of the Court, and that the deciding vote in *O'Connor* was cast by Justice Scalia, who rejected the idea of a discrete Fourth Amendment analysis to govern employer-employee searches, and instead argued that the law that governs workplace privacy in the non-government sector should apply as well to the government workplace.[298] The *Quon* majority explained why it would not resolve that issue in *Quon*,[299] and then proceeded to apply the *O'Connor* plurality approach to the facts of the case anyway.[300]

---

[296] Perhaps the technology exists which could interrupt any message I send to an employee of a government agency or private entity, informing me that all messages sent from or to that entity's system are subject to review by the entity, and asking whether, knowing this, I still want to send the e-mail or text message to Z.

[297] *See* Part III, introductory paragraph.

[298] City of Ontario v. Quon, 130 S. Ct. 2619, 2628 (2010).

[299] *Id.* at 2629.

[300] *See supra* Part III.E.2.

As a result, litigants and lower courts now must in essence litigate and decide the expectation of privacy issue twice: first they must address the facts of the case as if the *O'Connor* plurality approach was the law; second, they must do the same employing the approach Justice Scalia espoused in his *O'Connor* and *Quon* concurrences. Indeed, courts have begun to do so.[301] Fortunately, in the overwhelming majority of cases, the results will be the same under both approaches, because the law governing privacy issues in the non-governmental workplace is nearly indistinguishable from the Fourth Amendment approach outlined by the *O'Connor* plurality.[302]

As to the second issue, there are two compelling reasons why the Court was probably wise in declining to issue a broad ruling applying the Fourth Amendment to the use of employer-supplied electronic communications media in the workplace. First, in resolving the privacy implications of modern communications technology, it is helpful to understand how the technology works, and at least some members of the Court apparently lacked this knowledge.[303] Second, the technology is so new, and is evolving so quickly, that society's attitudes and expectations with regard to them are far from settled. Congress, rather than the Court, is the branch of government best equipped to study and resolve such issues by legislation, which, unlike a constitutional decision by the Supreme Court, can be amended to adjust to changing conditions and expectations.

The facts in *Quon* suggested, but did not actually present, two additional issues. First, should the employer be held to a more exacting standard if its inquiry is based on suspicions of the employee's misconduct, than if its purpose is merely to review the efficacy of workplace rules or practices? The logical answer is: It depends on the nature of the alleged misconduct, and the strength of the suspicions.[304] Second, assuming the *employee* lacked a reasonable expectation of privacy, does the government agency nonetheless have any obligations regarding the privacy expectations of those with whom the employee communicated? A plausible argument exists that the agency should take reasonable steps to assure that the non-employee participants in the communication are informed of the non-private nature of the communication.[305]

---

[301] *See, e.g.*, True v. Nebraska, 612 F.3d 676, 681-82 (8th Cir. 2010); Richards v. Los Angeles, 775 F. Supp. 2d 1176, 1182-86 (C.D. Cal. 2011).

[302] *See supra* Part IV.A.3.

[303] *See supra* Part III.E.3.

[304] *See supra* Part IV.B.

These are questions of some significance. In the absence of congressional action (or a Supreme Court decision), private and public sector employers are in essence resolving them unilaterally, by requiring, as a condition of employment, that employees acknowledge that they lack an expectation of privacy regarding their use of employer-supplied communications equipment and media.[306] Perhaps ultimately this is good public policy—it assures that employers can intervene to prevent misuse of their communications media, and it puts employees on notice regarding personal use such equipment. As the *Quon* majority acknowledged, moreover, most people have ample opportunity to communicate without employer oversight by using their own personal computers, cellular phones, and "smart" phones with texting and Internet access, the price of which are now well within the reach of most Americans.[307] But privacy is a fundamental and cherished right in this country.[308] Those of us who are employed tend to spend roughly half of our weekday waking hours at work.[309] It is disquieting that our right to privacy during such an important and substantial part of our lives is being decided solely by our employers, based on what they perceive to be their own self-interest.

---

[305] *See supra* Part IV.C.

[306] *See supra* Part IV.A.4.

[307] City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010); *see supra* Part IV.A.1. Inevitably, however, people who do own their own computers and smart phones will occasionally use office equipment to communicate on private matters.

[308] There are those among us who have renounced privacy and have chosen to share intimate details of their lives on the Internet, and some who, to the extent possible, live in front of video cameras. For my own rather dyspeptic view of these developments, see Clifford S. Fishman, *Technology and the Internet: The Impending Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations and the Media*, 72 GEO. WASH. L. REV. 1503, 1511-15 (2004).

[309] This assumes that the average fully employed person is awake seventeen hours a workday and spends roughly 8.5 hours on the job. Given that many employees are now electronically accessible for work-related matters during their supposedly "off" hours, the latter estimate may be low.

Not so long ago, Congress had the interest and energy to consider issues like these, and the ability to make the difficult choices and compromises necessary to resolve them.[310] Unfortunately Congress in 2012 has not displayed any of these characteristics, and there is little immediate reason for confidence that it will soon acquire them. The likely result is that individual privacy in the workplace will erode, quietly, bit by bit, without the public attention and study the matter deserves. Although the Court was correct in declining to issue a broad, sweeping decision, the decision had done little to reverse or impede that erosion.

APPENDIX. *QUON*: A USER'S MANUAL

The Court's restraint in *Quon*, however appropriate it may have been under the circumstances, leaves litigators and lower courts with significant questions as to how to proceed in new cases that arise involving workplace privacy. The outline that follows may prove useful in any attempts to follow the holding in *Quon*, when a government employee sues, alleging that the agency for which he or she worked violated his or her workplace privacy under the Fourth Amendment. I make no claim that it is an "open sesame" that will ineluctably lead to a winning argument or reversal-proof decision. I hope, however, that it will give litigants and courts a structure that will assure that all relevant issues and arguments are considered.

A. Determine whether the investigation clearly did, or clearly did not, intrude into an employee's (E) reasonable expectation of privacy

Logically, the first issue to address is whether a "search" under the Fourth Amendment occurred at all. If it did not, then E has no Fourth Amendment claim,[311] and is unlikely to have a common law invasion of privacy claim under state law, either. Often this issue is easy to resolve applying both the *O'Connor* plurality and Scalia concurrence approaches.

---

[310] Congress did so in 1968, when it enacted Title III, and in 1986 when it enacted the Electric Communications Privacy Act, and has amended each statute several times since, as in the U.S.A. PATRIOT Act and subsequent legislation. Congress did likewise when it enacted the many provisions designed to protect computer integrity and privacy. For an overview of such legislation, see FISHMAN & MCKENNA, *supra* note 10, §§ 1:10-1:21, 1:23.

> 1. Some information-gathering methods clearly *are* intrusions. Examples: physically searching E's desk, file drawers, office, and personal property within E's office;[312] concealing a microphone or camera in E's private workspace, without advance notice to E.[313] If there clearly was a Fourth Amendment search or a tort law intrusion, proceed to Part C.
>
> 2. Some information-gathering methods clearly are *not* intrusions. Examples: a supervisor standing in the hallway overheard what E said in his office. As Justice Stewart said in *Katz*, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[314] The same is probably true if E negligently exposed the information—for example, by leaving personal documents in the company photocopier.[315] If no such intrusion occurred, then render judgment for the defendant on the Fourth Amendment and pendant intrusion upon solitude claims.[316]
>
> 3. If (as in *Quon*) it is unclear whether the agency's actions intruded into E's reasonable expectation of privacy, the court should then consider whether, as in *Quon*, it can duck that issue by assuming there was such an intrusion, and evaluating whether that intrusion was reasonable under the circumstances. See Part C, *infra*. If, as in *Quon*, the answer to

---

[311] Because the Fourth Amendment protects only against unreasonable searches and seizures, if no "search" has occurred, *see supra* Part I.A.1, plaintiff has no Fourth Amendment basis on which to complain.

[312] *See supra* Part II.B.

[313] In *O'Connor*, a majority of the Court concluded that, barring unusual circumstances, an employee does have a reasonable expectation of privacy in his or her office. *See supra* Part II.B. Surreptitious electronic surveillance of private space is a per se intrusion into that expectation. Electronic surveillance issues are discussed further in Part D and E of this appendix.

[314] Katz v. United States, 389 U.S. 347, 351 (1967).

[315] There is no reason that the Fourth Amendment or tort law should protect someone from his or her own negligence or inattention.

[316] If the agency made improper use of the information, plaintiff may still have state law claims for intentional infliction of emotional distress, etc. *See supra* notes 244-46.

the latter question is "Yes," then judgment is rendered for the defendant as to the Fourth Amendment and intrusion upon solitude claims.

4. If it is necessary to resolve the reasonable expectation of privacy issue, move on to Part B.

B. Resolving whether the agency intruded upon E's reasonable expectation of privacy—in general

A number of factors must be considered, including:

1. Did the agency have a published policy concerning privacy or monitoring that covered its conduct in the case?

    a. How widely publicized was it; did E have actual or, at least, constructive notice?

    b. Does the policy clearly incorporate the type of monitoring, review or surveillance that was conducted in E's case?

    c. Was E given any "unofficial" or "off-the-record" assurance that the policy would not apply in his or her situation?

    d. Do compelling factual or social policy reasons exist for ruling that E had a reasonable expectation of privacy despite being on notice that he or she did not?

2. Assuming the issue is not resolved in Part B.1:

    a. Apply the *O'Connor* plurality approach. Given "[t]he operational realities of the workplace,"[317] did E have a subjective expectation of privacy against the investigative conduct by the agency? If so, is that expectation one society accepts as reasonable? Useful sources include leading treatises on the Fourth Amendment.

    b. Apply Scalia's *O'Connor-Quon* concurrence approach, i.e., the law governing the tort of intrusion upon solitude in the workplace, which differs little from the *O'Connor* plurality approach set forth in the preceding paragraph.[318]

---

[317] *O'Connor*, 480 U.S. at 717.

C. If there was an intrusion into E's reasonable expectation of privacy: Determine whether the intrusion was reasonable (or unreasonable) as a matter of law, or whether that is an issue for the jury.

Reasonableness is based on a variety of factors:

1. The goals and subject matter of the agency's investigation of E.

    a. If the agency conducted its search or inquiry to enable it to fulfill its public policy responsibilities, a plausible argument exists (for whichever party it favors) that *only* the *O'Connor* two-step approach should apply, because (the argument goes), the case falls into a different "special needs" category than the employer-employee category. Example: the urine sample tests for law enforcement officials upheld in *National Treasury Employees Union v. Von Raab.*[319]

    b. If the agency E worked for is not a law enforcement agency and the search was initiated and conducted by a law enforcement agency seeking evidence of criminal conduct, then the traditional Fourth Amendment requirements (probable cause that a crime was committed and, probably, a search warrant), not the "special needs" standard, should apply.[320]

    c. If the agency E worked for is not a law enforcement agency and E was suspected of conduct that might be criminal but the search was conducted by the agency for which he worked, the presumption should be that the primary purpose of the investigation is to further administrative or workplace goals, in which case the "special needs" rule set forth in C.1.d, *infra*, should apply.

---

[318] Useful sources include L. CAMILLE HEBERT, 1 EMP. PRIVACY LAW § 8:13; RICHARD E. KAYE, CAUSE OF ACTION TO RECOVER DAMAGES FOR INVASION OF PRIVATE SECTOR EMPLOYEE'S PRIVACY BY INTRUSION UPON SECLUSION, 42 CAUSE OF ACTION 2D 255 §§ 4-5 (2007); and, once it is published, chapter seven of the RESTATEMENT (THIRD) OF EMPLOYMENT LAW. No doubt there are others.

[319] 489 U.S. 656 (1989). See *supra* note 122 for further discussion of *Von Raab.*

[320] Note that this applies only if E has established that what was done constitutes a search. If E was on notice that he had no expectation of privacy in his office e-mails, for example, the fact that the agency turned them over to a law enforcement official who requested them does not create an expectation of privacy in those messages.

d. If the investigation was clearly intended to further workplace goals unrelated to broader public policy concerns and did not involve allegedly criminal activity, apply both the *O'Connor* plurality approach and Justice Scalia's tort-and-employment law approach to each information-gathering method which intruded into E's reasonable expectation of privacy.

2. Applying the *O'Connor* plurality approach:

a. Assess how important it was to the agency to obtain the information, how important it was to obtain the information promptly, and (where applicable) how important it was to obtain the information without notice to E. Within these parameters, afford high importance as to whether the agency's actions were an "efficient and expedient way" to obtain the needed information.[321]

b. Assess whether E's expectation of privacy was extensive, or only limited. *Quon* and *O'Connor* provide examples at the opposite ends of the spectrum. Compare what the Court categorized as Sgt. Quon's only limited (at best) reasonable expectation of privacy in his text messages, because as a police officer he should have known that they could be reviewed for a variety of reasons,[322] with Dr. Ortega's obvious and quite strong expectation of privacy in his office, desk and file drawers, particularly items that were obviously non-work-related papers and highly personal.[323]

c. Consider whether, when they conducted their search, the investigators reasonably expected to come across highly personal information, or not. If they reasonably did not expect to discover highly personal information, this is a significant factor in favor of reasonableness, even if they in fact learned highly personal information as a result.[324]

---

[321] City of Ontario v. Quon, 130 S. Ct. 2619, 2631 (2010).

[322] *See supra* Part III.E.2.

[323] *See supra* Part II.B.

d. The availability of less intrusive means is *not*, of itself, a controlling consideration (except, perhaps, in extreme cases), and a litigant or judge should say so three or four times to make it clear that the writer[325] knows that this is not a controlling consideration;[326] but it is a relevant consideration nevertheless. If a litigant or judge cites these other means, however, he or she should include a factually specific discussion as to whether each of these means would have enabled the agency to obtain the equivalent information with equal, or nearly equal, efficiency.

e. Did the agency make reasonable attempts to minimize the intrusion at the outset, and (if applicable) after they realized that they were discovering highly personal information?

(1) Did the searchers restrict where they looked, or how intensely they read or listened or watched? *O'Connor* and *Quon* again provide useful contrasts. In *O'Connor*, hospital employees examined, and seized, obviously personal items in which the hospital had no legitimate interest;[327] in *Quon*, the OPD requested transcripts of only two months of Sgt. Quon's text messages,[328] and the Internal Affairs officer assigned to the case read only the transcripts of messages Sgt. Quon sent and received while on duty.[329]

(2) If the searchers seized personal items of E that were of no legitimate interest to the agency, how long did the agency retain them before returning them? A court should not expect instantaneous

---

[324] The Court so held in *Quon*. *See supra* Part III.E.2.

[325] I mean here, the attorney writing a brief or the judge writing an opinion.

[326] I exaggerate here for effect. If the court in question is the Ninth Circuit, it should raise the ante to at least a dozen times. *See supra* note 189.

[327] *See supra* notes 90, 93 and accompanying text.

[328] *See supra* note 193 and accompanying text.

[329] *See supra* note 194 and accompanying text.

> evaluation and return of personal items that get swept up in the search, but prolonged retention aggravates the degree of intrusion.[330]
>
> (3) How many individuals were given access to personal information that was discovered during the search, and what use (if any) was made of such information? Once again, *O'Connor* and *Quon* provide useful contrasts. In *O'Connor*, the hospital used obviously personal information gleaned from the search to impeach Dr. Ortega's witnesses at trial;[331] in *Quon*, it appears that no unnecessary disclosures about the text messages occurred.[332]

f. In some cases, it will be clear, as a matter of law, that the agency's intrusion into E's privacy was reasonable.[333] In others, it will be clear as a matter of law, that the agency's intrusion into E's privacy was unreasonable.[334]

---

[330] *See supra* note 101.

[331] *See supra* note 101.

[332] *See supra* text accompanying note 195.

[333] The Supreme Court so held in *Quon*. *See supra* Part III.E.2.

[334] *See, e.g.*, Richards v. Los Angeles, 775 F. Supp. 2d 1176, 1176 (C.D. Cal. 2011). The L.A. Department of Public Works received an anonymous tip that one dispatcher, Richards, had engaged in sexual intercourse with a visitor when she was assigned, alone, to the dispatch room at night. *Id.* at 1179. To investigate this allegation, a camera was hidden in the dispatch room—a location with a locked door, no windows, and limited access, particularly at night, when the building was largely deserted. *Id.* at 1179-80 (The judge ruled that the circumstances gave dispatchers a reasonable expectation of privacy, *id.* at 1182, which seems correct given the facts.). The camera ran continuously for more than two months (until it was discovered by a dispatcher), recording the conduct of every dispatcher during that period. *Id.* at 1181. Dispatchers, when they were on duty alone, "engaged in a number of private acts in the dispatch room," including changing their clothing, pumping breast milk, picking zits, "and . . . other acts normally reserved for private spaces." *Id.* at 1180. The officer assigned to watch the videos was instructed to check out the behavior of all of the dispatchers, not just Richards's. *Id.* After the discovery of the cameras, the dispatchers sued. *Id.* at 1881. The judge held that the surveillance of the rest of the dispatchers (who were suspected of no wrongdoing) was per se unreasonable, and granted them summary judgment on that issue, a ruling that seems completely indisputable. *Id.* at 1185 (The judge held likewise for Richards—that ruling strikes me as somewhat debatable.).

g. In some cases, however, reasonableness under the circumstances will be a contested issue of fact, for the jury to resolve.[335]

3. Apply Justice Scalia's tort-and-employment law approach:

a. All of the factors in C.2.a through C.3.e logically would be relevant here, as well.

b. The ultimate question of fact, however, is somewhat different, or at least must be worded differently, because to succeed in a tort suit for intrusion upon seclusion, plaintiff must establish that, given all the circumstances, "the intrusion would be highly offensive to a reasonable person."[336]

D. Special circumstances—Claims involving "real-time" electronic surveillance: intercepting "wire, oral, or electronic communications"; video surveillance

1. Apply Parts A, B, and C, *supra.*

2. Keep in mind as well that if the employer's conduct constituted the "interception" (in essence, real-time monitoring, or recording) of the "contents" of a "wire, oral or electronic communication" by means of any "device," the conduct may constitute a felony in violation of 18 U.S.C. §2511(1), and may also be civilly actionable pursuant to 18 U.S.C. §2520, independent of any Fourth Amendment or common law claim.[337]

3. By contrast, there is no federal law that punishes or regulates the use of video surveillance. Thus, if such surveillance involved observation or recording only of E's physical conduct, without audio, a federal cause of action can

---

[335] The Supreme Court so held in *O'Connor*. *See supra* note 101.

[336] RESTATEMENT (SECOND) TORTS § 652B; *see supra* Part IV.A.3. Useful sources are suggested *supra* note 318.

[337] Each of the terms in quotation marks is defined in 18 U.S.C § 2510 (2006). For the definitions and their implications, *see generally* FISHMAN & MCKENNA, *supra* note 10, ch. 2. Many states have enacted similar statutes. For a detailed examination of crimes and civil actions relating to communications privacy, see *id.*, ch. 3. See also JAMES G. CARR & PATRICIA L. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE (2011), which also provides exhaustive coverage of these issues.

only be predicated on the Fourth Amendment, not on any federal statute.[338]

E. Claims involving review of stored electronic communications or use of office computers

1. Apply Parts A, B, and C, *supra.*

2. If the employer's conduct constituted unlawful accessing of stored electronic communications in violation of the SCA, the conduct may also constitute a crime in violation of 18 USC §2701(a), and may also be civilly actionable pursuant to 18 U.S.C. § 2707, independent of any Fourth Amendment or common law claim.[339]

3. If the employer's conduct involved surveillance of the employee's use of a computer, that may also provide a basis for a cause of action.[340]

4. Regarding the Stored Communications Act and the Computer Fraud and Abuse Act: if you are in the Ninth Circuit, *Theofel* and *Quon v. Arch Wireless* are controlling law; otherwise, although a party may cite them as persuasive authority, hopefully the judge will wisely decline to follow them.[341]

---

[338] For extensive coverage of these issues, see FISHMAN & MCKENNA, *supra* note 10, ch. 30.

[339] *See generally id.* ch. 7; *see also* CARR & BELLIA, *supra* note 337 (also providing extensive coverage of these issues); Orin S. Kerr, *A User's Guide to the Stored Communications Act—And a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

[340] *See generally* ORIN S. KERR, COMPUTER CRIME LAW (2d ed. 2009); FISHMAN & MCKENNA, *supra* note 10, chs. 21-27, which includes an exhaustive examination of all federal and state legislation on the subject.

[341] *See supra* note 158.